أطروحة الماجستير في علم الاجتماع التطبيقي

بعنوان

"ضحايا الاحتيال الإلكتروني في المجتمع الإماراتي"

إعداد

ناهد علي سيار

الشارقة 2019م

سيار، ناهد علي

342.620999

- س ن. ض

- ضحايا الاحتيال الالكتروني في المجتمع الاماراتي / ناهد علي سيار .ـ الشارقة، الامارات العربيه المتحدة: مركز بحوث الشرطة، ٢٠١٩ص ؛ ٢٤ سم (مركز بحوث الشرطة ؛ ٢١٧)

يحتوي على مراجع

١- الانترنت - قوانين وتشريعات ٢- الحاسبات الالكترونيه - قوانين وتشريعات

٣- الاثبات (قانون) ٤- الجريمة والمجرمون - الامارات العربية المتحدة

أ- العنوان

ISBN 978-9948-36-358-3

تمت الفهرسة بمعرفة مكتبة الشارقة

مادة الإصدارات تعبر عن آراء كاتبيها
وليس بالضرورة عن رأي مركز بحوث الشرطة

حقوق الطبع محفوظة لشرطة الشارقة / مركز بحوث الشرطة

الطبعة الأولى 1441هـ – 2019م

ص. ب: 29 ، الشارقة – الإمارات العربية المتحدة

هاتف: 5945112 – 009716 براق: 5382013 – 009716

E-mail: prc@shjpolice.gov.ae Website : www.shjpolice.gov.ae

بسم الله الرحمن الرحيم

قال تعالى:

الذين آمنوا ولم يلبسوا إيمانهم بظلم أولئك لهم الأمن وهم مهتدون

سورة الأنعام / الآية (82)

التوجه الاستراتيجية لوزارة الداخلية

2017 - 2021م

- **الرؤيــة :**

أن تكون دولة الإمارات العربية المتحدة من أفضل دول العالم في تحقيق الأمن والسلامة.

- **الرسالـة :**

أن نعمل بفاعلية وكفاءة ولتعزيز جودة الحياة لمجتمع الإمارات من خلال تقديم خدمات الأمن والسلامة بطرق ذكية وبيئة محفزة للابتكار وذلك حفاظا على الأرواح والأعراض والممتلكات.

- **القيــم :**

1- العدالة. 2- العمل بروح الفريق. 3- التميز والابتكار.
4- حسـن التعامل. 5- النزاهة. 6- الولاء.
7- المواطنة الايجابية.

- **الأهداف الاستـراتيجية :**

1- تعزيز الأمن والأمان.
2- جعل الطرق أكثر أمنا.
3- تعزيز السلامة والحماية المدنية.
4- ضمان الجاهزية والاستعداد في مواجهة الأحداث.
5- تعزيز رضا المتعاملين بالخدمات المقدمة.
6- ضمان تقديم كافة الخدمات الإدارية وفق معايير الجودة والكفاءة والشفافية.
7- ترسيخ ثقافة الابتكار في بيئة العمل المؤسسي.

يقوم مركز بحوث شرطة الشارقة بإصدار ونشر سلسلة من الدراسات في مختلف مجالات العمل الأمني والشرطي.

شــروط النشــر

1. الأصالة في مجال العلوم الشرطية والأمنية والتخصصات الأخرى ذات الصلة، وأن تكون الدراسة لم يسبق نشرها من قبل.

2. مراعاة قواعد وأصول البحث العلمي من حيث الأسلوب والنظرية والمنهج.

3. أن تتضمـن الدراسـة الرجـوع إلـى المصـادر العلميـة الحديثة.

4. أن تكتب الدراسة وتطبع بلغة عربية سليمة ويرفق معها ملخص باللغتين العربية والإنجليزية وألا يقل حجم الدراسة عن أربعين صفحة.

5. يلتزم الباحث بعدم إرسال دراسته إلى أي جهة أخرى للنشر حتى يصل إليه رد المركز وتعطى الأولوية للنشر حسب الأسبقية الزمنية للتحكيم.

6. لا يلتـزم المركز برد أصل الدراسة سـواء تـم نشـــرها أم لا.

7. تخضع الدراسات للتحكيم وتقرر الهيئة العلمية المشرفة على الإصدارات صلاحية الدراسة للنشر بناء على رأي ثلاثة محكمين متخصصين.

هيئة التحرير المشرفة على إصدارات
مركز بحوث شرطة الشارقة :

• المشرف العام : اللواء / سيف محمد الزري الشامسي
قائد عام شرطة الشارقــة

• رئيس التحرير : العميد الدكتور / خالد حمد الحمادي
مدير إدارة مركز بحوث شرطة الشارقة

• مدير التحرير : المقدم / عبدالله محمــد المليــح
رئيس قسم البحث العلمي
بمركز بحوث شرطة الشارقة

• الإشراف التنفيذي : النقيب / علي محمد بن هندي
مدير فرع البحوث الأمنية
بمركز بحوث شرطة الشارقة

• الإشراف الفني : المساعد/ أحمد أمين الزرعوني

أعضـاء الهيئـة العلمية المشرفة على إصدارات مركز بحوث شرطة الشارقة:

• المقدم/ عبدالله محمــد المليــح — رئيس قسم البحث العلمي بمركز بحوث شرطة الشارقة

• المقدم/ د. خليفة يوسف بالحاي — مكتب القائد العام

• المقدم/ د. عبدالله سيف الذباحي — مدير فرع الخدمات المساندة بمركز شرطة خورفكان الشامل

• الرائد/ د. جاسم بن جرش السويدي — مدير فرع التعليم الافتراضي بأكاديمية العلوم الشرطية بالشارقة

• الدكتور/ نواف وبدان الجشعمي — رئيس شعبة دراسات الجريمة بمركز بحوث شرطة الشارقة

تقديـــم

تمثل مناهج البحث العلمي السبيل الرئيسي لإقامة الحضارات واستباق الأمم. كما أنها تعد الأداة الأولى في تطويع تحديات الحاضر واستشراف المستقبل.

ويعد مركز بحوث شرطة الشارقة بالقيادة العامة لشرطة الشارقة أحد المراكز البحثية بالدولة والتي تتطلع بدور مهم في رصد كافة الظواهر الاجتماعية والأمنية وبحث أفضل الآليات للاستفادة من إيجابياتها ووأد سلبياتها لضمان استمرار ركب التنمية والتقدم ، كما يقوم المركز من خلال دراساته في مختلف جوانب الحياة الاجتماعية والقانونية والأمنية وبالتعاون والتنسيق مع المراكز البحثية الأخرى بالدولة وخارج الدولة بتقديم أفضل الحلول والمقترحات لكافة قضايا المجتمع.

وفي هذا الصدد تتعدد صور النشاط العلمي لمركز البحوث ما بين مؤتمرات وندوات وعقد دورات وحلقات ومحاضرات ومنشورات علمية ، وهو الأمر الذي يسهم بلا ريب في إثراء مجالات الفكر العلمي والأمني المختلفة وتقديم المشورة الفاعلة لمتخذي القرار وتوفير قاعدة علمية متميزة لكافة الباحثين والعاملين في مجالات العمل الاجتماعي والقانوني والأمني المختلفة للنهل منها وتقديم كل ما هو نافع ومفيد للحفاظ على مكتسبات المجتمع وأمنه.

والله ولي التوفيق،،،

اللواء / سيف محمد الزري الشامسي

قائد عام شرطة الشارقة

توطئـــة

في إطار تفعيل دور مراكز البحوث الأمنية ، يصدر مركز بحوث شرطة الشارقة مجموعة من الدراسات والبحوث في مجالات الأمن بمفهومه الشامل بهدف تكوين ثقافة أمنية لدى العاملين في الجهاز الشرطي، ودعم الدور المجتمعي في مجالات مكافحة الجريمة ، كما أنها وفي الوقت ذاته تمُد صاحب القرار الأمني بقاعدة بيانات علمية دقيقة تساعده في اتخاذ القرار السليم.

وتتضمن إصدارات عام 2019م عدداً من الدراسات والأبحاث المتميزة التي جاءت استجابة للتحديات الأمنية والمجتمعية وتصدياً للجرائم المستحدثة وملبية للتوجه الوطني والمؤسسي نحو التميز الاستراتيجي مواكبة للتطورات العالمية والمتمثلة في العولمة وإفرازاتها وتعالج قضايا أمنية وإدارية، بالإضافة إلى موضوعات قانونية واجتماعية.

وتتناول هذه الدراسة موضوع في غاية الأهمية خاصة في ظل انتشار الواسع للتكنولوجيا، إلا وهو مدى حجية التوقيع الالكتروني في الاثبات، وما يتعين على المشرع القيام به لمعالجة هذه المشكلة التي أصبحت واقعاً حتمياً.

نأمل أن تشكل هذه الدراسات بجانب الفعاليات العلمية التي يقدمها مركز بحوث الشرطة زاداً فكرياً ومعرفياً يعود بالنفع على كافة المواطنين والمقيمين في دولة الإمارات العربية المتحدة وفي أرجاء وطننا العربي والمهتمين والمختصين بهذا المجال.

العميد الدكتور / خالد حمد الحمادي

مدير إدارة مركز بحوث شرطة الشارقة

المحتويـــات

مستخلص 19

المقدمـــة 23

مصطلحات الدراسة 25

الفصل الأول: الخلفية النظرية 27

مشكلة الدراسة 27

تساؤلات الدراسة 29

أهداف الدراسة 30

أهمية الدراسة 30

الإطار النظري 31

نظرية نمط الحياة 32

الدراسات السابقة 35

منهج الدراسة 41

عينة الدراسة 41

أداة الدراسة 43

الفصل الثاني: تحليل النتائج 45

الفصل الثالث: مناقشة النتائج 87

الخاتمـــة 113

التوصيات 113

المراجع 115

الملاحق 119

مستخلـــــص

هدفت الدراسة بشكل رئيس للتعرّف على الخصائص الديموجرافية والاجتماعية والاقتصادية لضحايا الاحتيال الإلكتروني في المجتمع الإماراتي. ومحاولة التعرّف على العوامل التي أدّت بهم للوقوع ضحايا لهذه الجريمة، والكشف عن أنماط الاحتيال الإلكتروني الأكثر انتشارًا في المجتمع، ولتحقيق أهداف الدراسة فقد اعتمدت الباحثة على المنهج الكمّيّ والكيفيّ، وتم استخدام الاستبيان أداة رئيسية لجمع بيانات الدراسة علاوة على المقابلة، وطبّقت الدراسة على عيّنة عمدية بلغ حجمها 1830 مفردة تمثّل المجتمع الإماراتي تم الحصول عليها من إمارات: دبي، وأبوظبي، وعجمان، والشارقة، وأم القيوين، عيّنة إناث، وغالبية أفراد العيّنة في الفئة العمرية 18- أقل من 30 وفي مستوى البكالوريوس وأكثر نوع احتيال يتعرّض له أفراد العيّنة وأقاربهم يتمثّل في الاحتيال والنصب عبر الهواتف الذكية، ووجدت الدراسة أنّ أفراد العيّنة على وعي بأنواع الاحتيال الإلكتروني، كما وجدت الدراسة أن هناك دور للضحايا في تعرّضهم للاحتيال، وأنّ معظم الضحايا لا يبلغون بسبب جهلهم بأنّ القانون يحميهم. وقدّمت الدراسة عددًا من التوصيات؛ أبرزها التعريف بالمنظومة الحكومية التي يلجأ إليها المستهلك للتأكّد من مصداقية مواقع التسوّق الإلكتروني، وضرورة إيجاد برامج رسمية ومجتمعية توعويّة تهدف لتوعية أفراد المجتمع بمخاطر الاحتيال الإلكتروني وأنواعه، وإيجاد آلية رقابة حكومية على المتاجر الإلكترونية بكافة أنواعها.

وخلصت الدراسة إلى مجموعة من التوصيات، اهمها التدخّل التشريعي لمواجهة القصور في التشريعات والقوانين الجزائية أو تحديثها بالنص صراحة على تجريم الجرائم الإلكترونية والتعريف بنوعية الأدلة إعمالاً لمبدأ شرعية الجرائم والعقوبات حتى نصل إلى إقامة بنية قانونية للتصدي لمثل هذا النوع من الجرائم.

Victims of Electronic Fraud in the UAE

ضحايا الاحتيال الإلكتروني في المجتمع الإماراتي

The current study aimed at identifying the demographical, social, and economic features of the sample of the study. It also aimed at discovering the factors that led them to become victims of this crime, and identifying types of electronic fraud common in the society. The study applied the quantitative and qualitative methods and the questionnaire was used as a main tool for collecting study data as well as the interview. The study was applied to a non-probability sample of 1830 individuals representing the UAE society. The study found that the majority of the sample was females who were between the ages of 18 - less than 30. In terms of the educational level, the sample had a BA degree, and the most common type of fraud experienced was Smart Phone Fraud. The sample agreed that the victim played a role in fraud and that most victims didn't report this because of their ignorance of the fact that they are protected by the law. The study recommends creating a government body to which consumers can resort for ensuring the credibility of online shopping sites ; maintaining different types of close supervision on such electronic shops ; raising awareness of family members and checking donation websites whether inside and outside the UAE to make sure they are credible and reliable. Other recommendations also include: addressing shortcomings in penal legislations and laws or updating the same by expressly criminalizing cybercrimes, and defining required evidences in conformity with the principle of the legality of offences and penalties in a bid to combat such crimes.

المقدمة

تطوّرت الجريمة مع تطوّرات المجتمعات الإنسانية وتأثّر في تطوّرها مجموعة من المتغيرات الاجتماعية والاقتصادية والسياسية ومع كلّ حقبة زمنية تظهر أنواع حديثة من الجريمة، فظهرت الجرائم الإلكترونية التي تعدّدت أنواعها وأشكالها، ويعدّ الاحتيال الإلكتروني أحد أنواع الجرائم الإلكترونية (cyber crime) (marcum,2014) التي ظهرت في العقد السابع من القرن العشرين (1970) كان الاحتيال باستعمال الحاسوب من الجرائم الأولى التي بدأت تعرف على نحوٍ واسع على أنها نوعٌ جديد من الجرائم، ونتيجة لذلك تمّت أوّل مواجهة تشريعية لهذه الجرائم من خلال قانون فلوريدا لجرائم الحاسوب، فهو أوّل قانون جرّم الاحتيال على الحاسوب.

وقد صدر قانون فلوريدا في عام 1978م، وذلك بعد حادثة ذائعة الصيت في أحد الأحداث الرياضية حيث قام البعض بطباعة بطاقات مزوّرة. في ذلك الوقت تمّ تبني هذه المواجهة التشريعية من أغلب الولايات الأمريكية عدا ولاية فيرمونت.

ومع بداية الثمانينات، بدأت معظم حكومات العالم بسن قوانين مماثلة، فكانت كندا من أوائل الدول التي سنّت قانونًا اتحاديًّا يخاطب جرائم الحاسوب، وذلك عن طريق تعديل القانون الجزائي عام 1983م. كما صدر القانون الأمريكي للاحتيال وإساءة استخدام الحاسوب في عام 1984م، وتم تعديله في الأعوام 1986-1988-1989-1990م.

كما صدر في بريطانيا قانون إساءة استخدام الحاسوب في عام 1990م الذي جرّم الاحتيال في الفصل الثالث منه، وفي بداية التسعينيات مع شيوع الإنترنت وظهور الويب، امتدّت جرائم الحاسب إلى الشبكة المعلوماتية، وأصبح التركيز منذ ذلك الوقت على جرائم الإنترنت، وبخاصة الاحتيال عبر الشبكة (الخن، 2011م، ص39)

وجريمة الاحتيال الإلكتروني في العصر الحديث أصبحت من أكثر الجرائم انتشارًا على المستوى العالمي، وأصبحت تمثّل تهديدًا على الأمن الاقتصادي على مستوى

العالم وعلى الرغم من أهمية هذه الدراسة إلا أنها لم تحظ بنصيب وافر من الدراسات العلمية الجادة على المستوى العربي والعالمي، أمّا فيما يتعلّق بالضحايا فعلى مرّ العصور عانوا من التهميش العلمي حيث إنه في الماضي انصبّ كل الاهتمام على الجاني، وأحاطت العدالة الجنائية الجاني بسياج من الحقوق لصون كرامته، وتناست الضحايا وحقوقهم، الذي قام الجاني بسلب حقوقهم فتناست القوانين حقوق هؤلاء الضحايا في تعويضهم عن الأضرار النفسية والاجتماعية والاقتصادية التي يتعرّضون لها. فكان الاهتمام كله منصبًّا نحو الجاني وتوفير حقوقه كاملة نظرًا لتسليط الأضواء على حقوق المتّهم من قبل المدارس الفقهية العديدة، التي ركّزت جلّ اهتمامها عليه، وبسبب مناصرة الفلاسفة وحركات الدفاع عن حقوق الإنسان له (جاسم، 2015م).

وافتقر علم الجريمة إلى البحوث التي تدرس الضحايا مع أنهم هم المتضررون الأساسيون من الجريمة، فقد احتلّ المجرم بؤرة الاهتمام في هذه الدراسات سعيًا منها لفهم شخصيته والعوامل التي أدّت إلى ارتكاب الجريمة دون أن يوجّه الاهتمام الكافي للضحية على الرغم أنه المتضرّر الأساسي من الفعل والسلوك الإجرامي، ولكنه كان نسيًا منسيًّا. (هلال، 2005م)، (العموش، 2003م).

وأخيرًا بسبب تفاقم أعداد الضحايا الناتجة عن الكثير من الجرائم وتضاعف الأضرار النفسية والاجتماعية والاقتصادية التي تتسبّب بها على الضحايا، تمّ التوجّه النظري والتطبيقي للاهتمام لهؤلاء الضحايا والتوصّل إلى إيجاد حلول تكفل حماية حقوقهم. (Daigle, Leah E (Daigle, Leah E, 2013) ,(Daigle, leah E, 2012) ,2018).,

ويتمثّل الدافع الذاتي في الاهتمام بدراسة ضحايا الاحتيال الإلكتروني من خلال الواقع المعيش لطبيعة التكوين الاجتماعي والثقافي للمجتمع الإماراتي، فمع التطوّر التقني ازدادت جرائم الاحتيال الإلكتروني بشكلٍ كبيرٍ جدًّا.

وقد شكّل جميع المواطنين والمقيمين في المجتمع الإماراتي وحدة التحليل للتعرف على مدى إدراكهم لظاهرة الاحتيال الإلكتروني، وما هو دورهم في حدوث هذه الجريمة؟ وما هي العوامل المساعدة التي أدّت إلى زيادتها؟

مصطلحات الدراسة

الضحايا

الضحايا: الأشخاص الذين أصيبوا في ضرر فردي أو جماعي سواء بدني أم عقلي أم معاناة نفسية أم خسارة اقتصادية أم حرمان من التمتّع بالحقوق الأساسية عن طريق أفعال أو حالات إهمال تشكّل انتهاكًا للقوانين الجنائية. ويعرف العمر الضحايا: بأنه فرد أو تنظيم يمتلك أحد أو عناصر جاذبة تم إيقاعها في شبكة الاحتيال أو اغتصبت جنسيًّا أو حوّلت لرهينة لابتزازها. بتعبير آخر إنها نتاج صراع فردي (أو تنظيم مع أفراد) ينطوي على مضامين اجتماعية غير متكافئة وعلى قوى اقتصادية غير متوازنة (العمر، 2009م). يعرف الحربي ضحايا الجريمة: كلّ فرد تعرّض لسلوك إجرامي أو نمط إجرامي معيّن من طرف شخص أو مجموعة أشخاص نتج عنه إلحاق ضرر بدني أو نفسي أو اجتماعي أو اقتصادي به أو نتج عنه حرمان له من الحقوق التي تكفلها له التشريعات السماوية والقوانين الوضعية كإنسان له حقوق في مجتمعه أو خارج مجتمعه. (الحربي، 2011م). لأغراض الدراسة نعرّف الضحية: هو كلّ من تعرّض لضرر مالي نتيجة الاحتيال عليه بصور غير قانونية.

الاحتيال الإلكتروني:

الحيلة لغة: الاحتيال في اللغة العربية من الفعل الثلاثي (ح ي ل)، والحيلة اسم من الاحتيال، يقال ماله حيلة، وهو أحيل منه؛ أي: أكثر حيلة، وجريمة الاحتيال تعرف في اللغة الإنجليزية Fraud التي ورد تحديد معناها في قاموس مصطلحات العدالة الجنائية على أنها الحصول على النقود أو أي شيء آخر له قيمة عن طريق المظاهر الكاذبة والخداعة، وفي اللغة الفرنسية escroqurrie التي تعني النصب (الفيل، 574: 2012).

الاحتيال: هو سلب المال باستخدام طرق مبتكرة تعتمد على إيهام الجاني بغير الحقيقة وبأساليب المراوغة. (السلحدي، 2014م)

الاحتيال الإلكتروني: جريمة تتم باستخدام طرق احتيالية يوهم من أجلها المجني عليه بوجود مشروع كاذب، أو يحدث الأمل لديه بالحصول على ربح معلوماتي، أو من خلال تصرّف الجاني في المال، وهو يعلم أن ليس له صفة التصرّف فيه، باتخاذ اسم كاذب أو صفة كاذبة تمكّنه من الاستيلاء على مال المجني عليه، فيتم التحويل الإلكتروني للأموال من خلال اتصال الجاني مع المجني عليه عن طريق الشبكة أو التعامل المباشر للجاني مع بيانات الحاسب الآلي باستعمال بيانات غير حقيقية، والتي تساعده في إيهام الحاسب الآلي والاحتيال عليه فيسلمه النظام المال. (يوسف، 45:2013)

يعرّف الاحتيال من خلال النظرة الاجتماعية بأنه "سلوك تفاعلي يقــع بــين فردين يشتركان في فعل اجتماعي وأحد ولفترة قصير من الزمن، يكون أحدهما مستخدمًا أسلوب الاستمالة أو الإغراء (المحتال) مع طرف ثانٍ يشترك معه في فعل اجتماعي محدّد (الضحية) من أجل الحصول على مال أو شيء قيم يمتلكه، وذلك عن طريق الخداع أو الغشّ أو الكذب أو التحريف" (الفالح، 2006).

الجريمة الإلكترونية: هي الجريمة التي تتم بواسطة الحاسب الآلي أو بواسطة شبكة الإنترنت، وتتّسم بالسرعة وتطوّر وسائل ارتكابها وينعدم فيها العنف المادي ضد الإنسان بالمقارنة مع التقليدية أثناء تنفيذها، وهي عابرة للحدود، من سماتها أيضًا أنّ أدلّتها سهلة الإتلاف، كما أنّ الجهات التي تتولى تعقبها والتحقيق فيها تواجهه صعوبات وتعقيدات كثيرة وتنقصها أحيانًا الخبرة وعدم كفاية القوانين الخاصة بمعالجتها. (مجمع البحوث والدراسات، 2016م).

لأغراض هذه الدراسة نعرف الاحتيال الإلكتروني: كافة وسائل الاحتيال عن طريق الإنترنت بهدف الاستيلاء على المعلومات أو أموال المجني عليه بطريقة غير شرعية.

الفصل الأول
الخلفية النظرية

مشكلة الدراسة:

تكمن مشكلة الدراسة في خطورة هذه الظاهرة العالمية حيث أشارت التقارير العالمية إلى أنّ الجرائم الإلكترونية تكلف العالم ما يقرب من 600 مليار سنويًّا ووصلت عدد البلاغات عام 2017م إلى 4 ملايين بلاغًا حسب إحصاء مكتب التحقيقات الفيدرالية، وتتمثّل تقديرات ضحايا الجريمة الإلكترونية سنويًّا 556 مليون ضحية كلّ عام – 1.5 مليون ضحية كلّ يوم – 18 ضحية في الثانية – 232.4 مليون بطاقة هوية تتمّ سرقة معلوماتها – أكثر من 600 ألف حساب في الفيس بـــوك الاشتباه فيها، والاطلاع عليها يوميًّا 1 من كلّ 10 أشخاص من مستخدمي شبكات التواصل الاجتماعي يقعون ضحية لتواصل مشبوه (مجمع البحوث والدراسات، 2016م)، كشف تقرير نورتن سيماتتيك أنه بلغت تكلّفت الجرائم الإلكترونية في العالم في العام 2015م (150 مليار) دولار، أمّا في العام 2016م بلغت 126 مليار دولار حيث تضرّر 689 مليون شخص من الجرائم الإلكترونية، وفي العام 2017م تضرّر 978 مليون شخص في 20 بلد بسبب الجريمة السيبرانية حيث تأثّر 44٪ من المستهلكين بجرائم الإنترنت في الأشهر الــ 12 الماضية، وبلغت تكلفة الجرائم الإلكترونية على مستوى العالم 172 مليار دولار – بمتوسط 142 دولارًا لكل ضحية –وما يقرب من 24 ساعة على مستوى العالم . و على صعيد الخليج العربي كشف تقرير نورتن سيماتتيك في العام 2012 أن خسائر دول مجلس التعاون الخليجي من جراء جرائم المعلوماتية بلغت 850 مليون دولار، بينما تجاوزت الخسائر لدول الخليج ذاتها في العام 2013م مبلغ 900 مليون دولار، أمّا على صعيد المجتمع الإماراتي أظهر تقرير مختصّ بجـــرائـــم الإنترنت أنّ الهجمات الإلكترونيـــة في عـــالم الأعمال في الإمارات تسبّبت في خسائر

فاقت 422 مليون دولار في العام 2012م (مجمع البحوث والدراسات، 2016م) كشف تقرير نورتن سيمانتيك أن الهجمات الإلكترونيـــة في عـــالم الأعمال في الإمارات تسببت في خسائر كبيره حيث في عام 2015 بلغت 1.3 مليار دولار اما في عام 2016 بلغت 1.4 مليار دولار في حين بلغ في عام 2017م 1.1 مليار دولار، ونتيجة للخسائر الاقتصادية الكبيرة التي تسبّبها الجرائم الإلكترونية بشكلٍ عامّ والاحتيال الإلكتروني بشكلٍ خاصٍّ حيث يعدّ الاحتيال الإلكتروني أحد أنواع الجرائم الإلكترونية، وأيضًا تعدّدت أنواع الاحتيال الإلكتروني وأضراره فمن خلال الإحصائيات السابقة يلاحظ أنها جريمة عالمية تهدّد الأمن الاقتصادي العالمي، ومن ضمن المجتمعات التي تتأثّر في هذه الجرائم المجتمع الإماراتي، وبالنظر لعدد البلاغات في مدينة دبي للضحايا الذين تعرّضوا للاحتيال الإلكتروني في عام 2016م فوصل عدد البلاغات إلى 230 بلاغ في حين في عام 2017م وصل 205 بلاغات، وصنّفت إلى الصور التالية: ففي عام 2016م وصلت بلاغات التهديد والابتزاز عبر الإنترنت 23. أمّا في عام 2017م وصلت عدد البلاغات 32، وبالنسبة للاستيلاء عن طريق استخدام تقنية المعلومات في عام 2016م وصلت البلاغات 193، أمّا في عام 2017م وصلت 163، وأمّا استخدام بيانات بطاقة ائتمانية أو غيرها من البطاقات الإلكترونية بغير وجه حق عن طريق تقنية المعلومات في عام 2016م وصلت لـــ 13 بلاغ، أمّا في 2017م وصلت لـــ 9 بلاغات، أمّا بالنسبة للوصول لبيانات بطاقة ائتمانية أو غيرها من البطاقات الإلكترونية بغير وجه حقٍّ عن طريق تقنية المعلومات في عام 2016م كانت 1 بلاغ وفي عام 2017م، 1 بلاغ (قسم الجرائم الإلكترونية، القيادة العامة لشرطة دبي، إحصائية غير منشورة) فانتشار الاحتيال الإلكتروني وازدياده ربما يعود إلى التطوّر في جميع المجالات وسرعة إنجاز المعاملات، والزيادة السكانية الكبيرة في المجتمع، إضافة إلى تعدّد الأديان والجنسيات، فشهد المجتمع تحوّلات كبيرة في الجوانب الاقتصادية والاجتماعية والسياسية، الأمر الذي أدّى إلى تفاقم ظاهرة الاحتيال الإلكتروني وازديادها.

والعوامل الآتية تزيد من حدّة وتعقيد مشكلة البحث: حيث يعدّ الاحتيال الإلكتروني من الجرائم المستحدثة التي تتمّ عن طريق الإنترنت، ومن الصعب إيجاد دليل على المجرم أو القبض عليه أو معرفته في بعض الأحيان، بالإضافة إلى صعوبة مكافحة جرائم الاحتيال الإلكتروني بسبب سهولة إخفاء معالم الجريمة، وصعوبة الحصول على دليل، وجرائم الاحتيال الإلكتروني تعمل على تهديد الأمن الاقتصادي والتجارة الإلكترونية وعدم الثقة بين الناس في إنجاز معاملاتهم، بالإضافة إلى أنّ المجرمين يقومون بالاستيلاء على البيانات الشخصية في الحاسب الآلي أو الهواتف النقالة، واستخدامها ضدّ الضحية أو استغلالها بغير وجه حقّ، ويلاحظ في الآونة الأخيرة ارتفاع معدلات الاحتيال الإلكتروني على المستوى الإماراتي وعدم دراستها نظرًا لغياب الإحصائيات الدقيقة، فمع ازدياد الاستخدام للإنترنت ازدادت جرائم الاحتيال عبر الإنترنت، ورغم الإدراك بخطورة ظاهرة الاحتيال الإلكتروني وانتشارها إلا أنه لم يحظ بالاهتمام والتفسير والتحليل في دراسات علم الجريمة.

تساؤلات الدراسة:

1. هل أفراد العينة على دراية ووعي بأنواع الاحتيال الإلكتروني؟
2. ما أنماط الاحتيال الإلكتروني التي سبق وتعرّض لها أفراد العينة، وما الأنماط التي سبق وأن تعرض لها أقرباء أفراد العينة وأصدقاؤها؟
3. هل يختلف تعرّض أفراد العيّنة للاحتيال الإلكتروني حسب كلّ من متغيرات: (النوع، والعمر، والمستوى التعليمي، والجنسية، استخدام برامج التواصل الاجتماعي والتسوق الإلكتروني)؟
4. ما هو دور أفراد العينة في تعرّضهم للاحتيال الإلكتروني؟
5. هل يقوم أفراد العيّنة بالإبلاغ عند تعرّضهم للاحتيال؟ وما الأسباب التي تحول دون إبلاغهم، وهل هم على دراية بالقوانين التي تكفل حقّهم في حال تعرّضهم للاحتيال الإلكتروني؟

أهداف الدراسة:

تهدف هذه الدراسة إلى التعرّف على ضحايا الاحتيال الإلكتروني في مجتمع الإمارات، وعلى النحو الآتي:

1. التعرّف على وعي أفراد العينة بأنواع الاحتيال الإلكتروني.
2. التعرف على أنماط الاحتيال الإلكتروني التي سبق وتعرّض لها أفراد العيّنة في الفترة السابقة: في آخر 12 شهر أو منذ سنتين ومنذ أكثر من ثلاث سنوات والتي تتضمّن: الخبرة31 المباشرة للضحايا Direct Victimization. والخبرة السابقة Former Victimization والتعرّف على أنماط الاحتيال الإلكتروني التي سبق وتعرض أقارب أفراد العينة وأصدقاؤهم.
3. التعرّف على دور أفراد العيّنة في تعرّضهم للاحتيال الإلكتروني.
4. التعرّف على العلاقة بين المتغيّرات الآتية (الجنس، العمر، المستوى التعليمي، الجنسية، استخدام برامج التواصل الاجتماعي، التسوق الإلكتروني) والتعرّض للاحتيال الإلكتروني.
5. التعرّف على ثقافة أفراد العيّنة بأهمية الإبلاغ عند تعرّضهم للاحتيال والتعرف على الأسباب التي تحول دون إبلاغهم، والتعرّف على وعي أفراد العيّنة بالقوانين التي تكفل حقّهم في حال تعرّضهم للاحتيال الإلكتروني.

أهمية الدراسة:

احتلّ موضوع ضحايا الاحتيال الإلكتروني أهمية كبيرة في علم الجريمة على المستويين النظري والتطبيقي لما لهذا المهدّد من انعكاسات سلبية على التنمية البشرية المتنامية.

على المستوى النظري: تتمثّل الأهمية العلمية فيما ستقدّمه للتراث العلمي المعرفي حول ضحايا جرائم الاحتيال الإلكتروني حيث تعدّ هذه الدراسة من الدراسات الحديثة التي تهتم بدراسة ضحايا الاحتيال الإلكتروني، ويلاحظ قلة وندرة في الدراسات في هذا الجانب نظرًا لحداثة موضوع ضحايا جرائم الاحتيال الإلكتروني كونه يعتبر من الجرائم المستحدثة، وحسب علم الباحثة تعتبر هذه الدراسة من الدراسات الأولى التي طبّقت على المجتمع الإماراتي، وتعدّ محاولة علمية لإثراء حقل علم ضحايا الجريمة في جريمة مستحدثة بأسلوبها وأنواعها وطرق تنفيذها، وفي ضوء ذلك فإنّ هذه الدراسة سوف تنطلق من نظرية أنماط الحياة والنوافذ المحطمة وتصنيف ضحايا الاحتيال.

على المستوى التطبيقي: تمثلت الأهمية التطبيقية فيما ستقدمه الدراسة الحالية لصناع القرار من معلومات مهمة ومفيدة حول ضحايا الاحتيال الإلكتروني، ويمكن أن تفيد وزارة الداخلية في تقديم معلومات حول خصائص ضحايا الاحتيال الإلكتروني والأنواع التي يجهلها أفراد المجتمع، وحجم انتشار الظاهرة، وأكثر الأنواع التي يتعرض لها أفراد المجتمع والعوامل المساهمة في زياده الضحايا، وأيضًا تتمثل الأهمية في زيادة الوعي المجتمعي في أنواع الاحتيال الإلكتروني نظرًا لارتفاع معدلات الضحايا وانتشار هذه الظاهرة، ومن الممكن أن تسهم الدراسة في بعض جوانبها في وضع برامج وقائية للحدّ من هذه الظاهرة.

الإطار النظري

سوف تتناول الدراسة في هذه الجزئية النظريات المفسرة لوقوع الأفراد كضحايا لجرائم الاحتيال الإلكتروني، ويتم ذلك من خلال النظريات الآتية:

أولاً: نظرية النوافذ المحطمة

ثانيًا: نظرية نمط الحياة

ثالثًا: نظرية تصنيف الضحايا حسب مساهمة الضحية في وقوع الفعل الإجرامي

نظرية النوافذ المحطمة:

من أشهر نظريات الوقاية من الجريمة (Keling and Coles,1996)، وتقوم هذه النظرية على فكرة الإهمال، والذي يؤدي إلى خلق الظروف المناسبة للجريمة، وعلى سبيل المثال إذا قام أحد بكسر نافذة فإن هذا يشجع الآخرين على تحطيم نوافذ أخرى، وهذا يعطي المجرم الفرصة والوضع المناسب لارتكاب الجرائم. (العموش، 2003م)

فصطلح النوافذ المحطمة ينصّ على أنه مثلما تركت نافذة مكسورة بدون دلالة، فهذا سيجعل المارة يظنون أن لا أحد يهتم ممّا سيؤدي إلى تحطيم مزيد من النوافذ وانتشار الفوضى، وانتشار الخوف من الجريمة وانتشار الجرائم، حيث إنّ النافذة المحطمة تعدّ ثغرة لدخول الجاني (William H. Sousa, Ph.D.,2004)

نظرية نمط الحياة:

وتمحورت هذه النظرية حول سؤال الخطورة، والتي طوّرت من قبل مايكل هندلانج وآخرون (1978م) فقد أرادوا معرفة الأسباب التي تضع بعض الجماعات تحت الخطورة وليكونوا ضحايا للجريمة دون غيرهم. ولقد توصّلوا إلى أن أنماط النشاطات أو نمـــط الحياة للأفراد يعرضهم بدرجات متفاوتة لاحتمالية أن يكونوا ضحايا محتملين، وكان جوابهم هو أن النشاطات المنمطة، أو أنماط حياة الأفراد، تقود إلى معدلات ضحايا مختلفة. وتمتاز أنماط الحياة هذه بأنها وظائف يومية تشمل نشاطات العمل ونشاطات أوقات الفراغ.

تتأثّر أنماط الحياة بثلاثة عناصر أساسية:

أولاً: الدور الاجتماعي الذي يمارسه الناس في المجتمع وبناء على توقّعات الآخرين، يتصرف الناس بطرق معينة وينشؤون أنماط حياة توصلهم إلى الوقوع ضحية للجريمة على نحو أكثر أو أقل.

ثانيًا: الموقع في البنى الاجتماعي كلما ارتفعت مكانة المرء، كلما قلت خطورة وقوعه ضحية للجريمة، وذلك بسبب نوع النشاطات التي ينخرط فيها المرء والأماكن التي يتردّد عليها.

ثالثًا: المكوّن العقلاني التي تتخذ إزاءه القرارات في تحديد السلوكيات المرغوبة. وبناء على الدور الاجتماعي للفرد ومكانته في البناء، فيمكن اتخاذ القرارات لتقييد السلوكيات الروتينية إلى سلوكيات آمنة نسبيًّا أو القبول بالمخاطرة. ويميل صغار السن بتعزيز احتمالية وقوعهم ضحايا من خلال اختيارهم الانخراط في نشاطات في زمان ومكان لها مستويات خطورة مرتفعة من مثل الذهاب إلى النوادي الليلية.

وعندما تؤخذ اختلافات نمط الحياة بالحسبان فإن خبرات الوقوع ضحية للجريمة واحتمالية الوقوع ضحية لها يمكن التنبؤ بها إلى حد كبير نسبيًّا. أمّا بالنسبة لهؤلاء الذين توجد خلفياتهم الاجتماعية والبنائية تفاعل أكبر مع المجرمين والأماكن المفضية إلى الجريمة، فيكونوا في الحقيقة في خطر أكبر في أن يكونوا ضحايا وبالمثل، فالأفراد من الطبقة الاجتماعية العليا والذين انخرطوا في نشاطات روتينية أقلّ (مثلاً لديهم نمط حياة) والتي تتضمّن بالتالي مواجهة أقل مع المجرمين على الأقل مجموعة مجرمين الشوارع ستكون احتمالية وقوعهم ضحية للجريمة أقل، ويمكن لمثل هذه المخاطر أن تزداد وتتناقص لتتخطى المستويات المتوقّعة عادة بالنسبة للجماعات التي ينتمي إليها الفرد، عن طريق القرارات الواعية التي يتّخذها الأفراد للانخراط في أنماط حياة معينة (Williams III, Frank and Marilyn D.McShane,2010)

نظرية تصنيف الضحايا حسب مساهمة الضحية في وقوع الفعل الإجرامي:

1. الضحية المتهور: تلك السلوكيات التي يرتكبها بعض الأفراد ويكون لها دورٌ كبير في وقوعهم كضحايا للجريمة. وهذا سلوك أرعن يقدم عليه الفرد وقد

ينجم عنه أن يتعرض للوقوع ضحية للجريمة من جراء ذلك السلوك، ومفهوم التهور هو حالة الشخص الذي يقوم بسلوك أو تصرف لا يحسب ولا يقدر نتائجه (سلوك طائش)، ممّا يؤدّي إلى وقوعه ضحية للجريمة. (الحربي، 2011م)

2. الضحية المسهل؛ أي: أن يقوم الفرد بإجراء يسهل للمجرم الإيقاع به ويأخذ النوع من الضحايا عدة أشكال، منها أن يدخل الفرد في محيط اجتماعي أو ثقافي أو بيئي لا يعرفه مسبقًا ولا يعرف ما يمكن أن يحيط به من مخاطر من جراء دخوله في هذا المحيط، هذه العملية تسهل الإيقاع بالفرد ضحية لجرائم متنوعة ومتعددة. (الحربي، 2011م)
3. الضحية المولع بالاكتساب: هذا الصنف يوجد في جميع فئات المجتمع فالفقير يريد توفير الحاجات الأساسيات، ومتوسط الحال يريد الحصول على الكماليات، والغني يطمح إلى مضاعفة ثروته. (الحربي، 2011م)
4. الضحية المهمل: يقصد بالإهمال حصول الخطأ بطريق سلبي نتيجة لترك واجب أو الامتناع عن تنفيذ أمر ما. فالضحية هنا يغفل اتخاذ احتياط يوجبه الحذر وتمليه الخبرة الإنسانية على من كان في مثل ظروفه، كمن يترك سيارته مفتوحة الأبواب وبها أشياء ثمينة، أو من يترك منزله دون إحكام إغلاقه في حال قيامه بالسفر خارج البلاد. (أحمد، 2011م)

الدراسات السابقة:

من خلال مسح للأدبيات والدراسات السابقة فقد تبيّن أنّ موضوع الدراسة يعاني من ندرة في الدراسات ذات العلاقة المباشرة به، ولكن تم العثور على بعض الدراسات التي من الممكن أن تفيد حول موضوع الدراسة.

كشف المسح الوطني لضحايا الجريمة في المجتمع الأمريكي (NCVS,2017)، خصائص الضحايا وأنواعهم كضحايا الملكية وضحايا الاغتصاب، ويطبّق سنويًّا المسح على 220.000 شخص.

أشارت دراسة (مركز البحوث والدراسات، 2016م) حول الجريمة الإلكترونية في المجتمع الخليجي، وكيفية مواجهتها إلى الاستخدامات السلبية لشبكات التواصل الاجتماعي، وتمثّلت في:

1. بثّ الأفكار الهدّامة والدعوات المنحرفة والتجمّعات المخالفة للقيم والقانون.
2. عرض المواد الإباحية والفاضحة الخادشة للحياء العام.
3. التشهير والمضايقة وبثّ الإشاعات.
4. التحايل والابتزاز والتزوير.
5. انتهاك الحقوق الخاصة والعامة.
6. الاستغلال الجنسي للأطفال.

وأشارت إلى النتائج الآتية: -تأكّد أنّ الجريمة الإلكترونية ظاهرة إجرامية حديثة وليدة التطورات الهائلة والمتلاحقة في نظم تقنية المعلومات والاتصالات، وهي جريمة عابرة للحدود يمكن ارتكابها من أيّ مكان في العالم عبر شبكة الإنترنت، وتتميّز بسهولة إخفاء أدلّتها، إضافة إلى تعقيدات التحقيق فيها وصعوبة ضبط مرتكبيها، وصارت مشكلة عالمية تهدّد أمن المجتمع الدولي، وارتفعت معدلات الجريمة

الإلكترونية بشكلٍ ملحوظ منذ عقد التسعينات من القرن الماضي، وفي عام 1997م قامت مجموعة الدول الثمانية G-8 بالتحرّك الدولي لمواجهة الأزمة.

أشار (العنزي، 2016م) في دراسته حول الحماية الجنائية للمجني عليه من الابتزاز أن ما يساعد على جريمة الابتزاز، سهولة التواصل بين الجنسين عبر وسائل التقنية المختلفة، ما ينتج عنه في الأخير اعتداء على حرمة الحياة الخاصة للفرد عن طريق الحصول على معلومات تخصّ المجني عليه تكون سلاحًا بيد المبتزّ يسـلّطه على الضحية كلما أراد تحقيق نتيجة لصالحه.

أجرى الزهراني، (2014م) دراسة وصفية عن جريمة الاحتيال الإلكتروني في النظام السعودي، وأظهرت نتائج الدراسة: تعد السمات الشخصية لكلّ من الجاني والمجني عليه أهم العوامل التي تساعد على انتشار جريمة الاحتيال الإلكتروني. وكشفت نتائج الدراسة أن المعاهدات والاتفاقيات الدولية تمثّل مصادر مهمّة للتشريعات الوطنية لمكافحة جرائم الاحتيال الإلكتروني. وأنّ النظام السعودي أو القانون الإماراتي لم يتناول وسائل الإثبات التي يمكن الاعتماد عليها في إثبات جريمة الاحتيال الإلكتروني، كما لم يحدد النظام السعودي أو القانون الإماراتي سبل التنسيق مع الدول الآخرى، وحالات تنازع القوانين أو الاختصاص القضائي.

أشارت دراسة (Daigle,leah E ,2012) ، (Daigle,Leah E ,2013) إلى بيان عوامل الضحايا ونتائجه وحقوق ومجالات الضحايا، ومن أبرزها ضحايا الاحتيال الإلكتروني.

أجرى (هلال، 2012م) دراسة عن ضحايا الجريمة: دراسة اجتماعية على عينة من ضحايا جرائم السرقة، أن أغلب ضحايا جرائم السرقة من الذكور وأعمارهم من 35- 50 وأغلبهم من المتزوجين، ويتراوح مستواهم التعليمي ما بين التعليم الإعدادي والثانوي، وأن 60% من الضحايا من الموظفين وبعد ذلك رجال الأعمال ويليه الحرفيون، وأن وقوع الجريمة ضدهم كان في ساعة متأخرة من الليل، وأنه لا يوجد

سابق معرفة بين الضحايا والجناة، وأخيرًا أوضحت النتائج بأن الضحايا قد عانوا من الاكتئاب والضيق والحزن والشعور بالدونية والنقص. كما أوضحت الدراسة أن هناك خسائر مادية لحقت بالضحايا من جراء جرائم السرقة تراوحت ما بين دخل الضحية الذي يتقاضاه شهريًّا إلى ما يتقاضاه في مدة شهرين أو ثلاثة شهور في بعض الحالات.

أشار (الحربي، 2011م) في دراسته حول ضحايا التهريب البشري من الأطفال، والتي استخدم خلالها نظرية أسلوب الحياة، حيث توصّل لعدد من النتائج أبرزها: إنّ تدني المستوى التعليمي للأفراد بشكلٍ عامٍّ يلعب دورًا في وقوعهم ضحايا، كما أثبتت الدراسة أن للأسرة وللفقر دور كبير في وقوع الأطفال كضحايا للجريمة.

أجرى الشمري، (2011م)، دراسة عن دور الضحية في حصول الفعل الإجرامي من منظور طلاب الجامعة –دراسة مسحية على طلبة جامعة نايف العربية للعلوم الأمنية-. وأظهرت نتائج الدراسة أن وجهة نظر طلبة جامعة نايف العربية للعلوم الأمنية حول دور الضحية في حصول الفعل الإجرامي كانت مرتفعة وبدرجة عالية، وقد احتلّ بعد دور الاستفزاز (من قبل الضحية) المرتبة الأولى، يلي ذلك دور طبيعة سلوك الضحية، ثم يليه دور المتغيرات الشخصية للضحية، وفي المرتبة الأخيرة سمات الضحية، في حصول الفعل الإجرام.

أجرى (المطيري، 2008م) دراسة حول خصائص ضحايا جرائم الاحتيال المالي على عيّنة من الضحايا بمدينة الرياض، وأشارت الدراسة إلى النتائج الآتية: 1- إنّ الذين تتراوح أعمارهم ما بين (36-45) أكثر الفئات تعرّضًا للاحتيال، وإنّ مكان النشأة للضحايا هو القرى، والمستوى التعليمي للضحايا هو المستوى المنخفض وتعليمهم ثانوي فأقل، وأغلب الضحايا متزوجون وموظفيون حكوميون مدنيون، والدخل الشهري للضحايا هو الدخل المرتفع (6001 فأكثر)، وأغلب الضحايا لا يملكون مسكنًا خاصًّا بهم ولا يمارسون نشاطًا تجاريًّا، وأغلب الضحايا عليهم قروض لمواطنين أو البنوك. 2- أكثر جرائم الاحتيال المالي انتشارًا في مجال توظيف الأموال.

3- أساليب الاحتيال التي تعرض لها الضحايا كالآتي: بالمرتبة الأولى: تقديم المحتال ضمانًا ماليًّا غير سليم، في المرتبة الثانية: الإيهام بربح مالي كبير وسريع، وبالمرتبة الثالثة: استعانة المحتال بشخص للتأثير عليك. 4- العوامل التي تؤدي لوقوع جرائم الاحتيال المالي: بالمرتبة الأولى العوامل المرتبطة بخصائص الضحية، في المرتبة الثانية: العوامل المرتبطة بطبيعة الجريمة، في المرتبة الثالثة: العوامل المرتبطة بقدرات الجاني.

الشوال (2008م) في دراسته حول اتجاهات طلبة جامعة الطفيلة التقنية نحو دور الضحية في وقوع الجريمة إلى النتائج الآتية: الجهل بالمحيط الاجتماعي يزيد من احتمالية وقوع الشخص ضحية للجريمة بمتوسط (3.64)، إنّ إهمال بعض الضحايا في التعامل مع ممتلكاتهم أدّى إلى سرقتها بمتوسط حسابي (3.62)، وإنّ عدم تعاون بعض الناس في الإبلاغ عن المجرمين يؤدي إلى زيادة أعداد الضحايا بمتوسط حسابي (3.56).

أجرى (العموش، 2008م) دراسة حول المشكلات الاجتماعية في الإمارات: وإنّ (89%) من المبحوثين يعانون من خطورة الجريمة، وقد بلغ متوسط عدد المشاكل التي يعاني منها الفرد الواحد (3.1%) مشكلة، في حين اختلف هذا المتوسط حسب جنسية المبحوثين، فقد كان متوسط عددها (4.4) مشكلة لكلّ مــواطن، وانخفض هذا المتوسط عند العرب إلى (3.04) مشكلة، فيما كان الانخفاض واضحًا عند الأجانب، فبلغ متوسطها (1.3) مشكلة. وقد كشف التباين الأحادي عن معنوية دلالة الفروق في المتوسطات.

وأشارت نتائج الدراسة إلى أنّ (15.0%) من أفراد العينة يخافون من الجريمة، والسرقة بأنواعها (28.3%)، وانتشار المخدرات (43.7%)، والمشروبات الكحولية (33.7%)، والإدمان (20.1%)، والغش التجاري (38.9%)، والنصب والاحتيال

(29.1%) ، والتزوير (15.7%)، وحوادث المرور (48.8%) ، والخوف من الشرطة، والاعتداء (الإيذاء البسيط أو البليغ) (13.4%)، والاغتصاب (15.7%).

وأظهرت نتائج الدراسة أنّ (34.75%) من الذكور يدركون أن الاغتصاب يمثّل أحد عوامل الخطورة في المجتمع المحلي، وانخفضت هذه النسبة إلى (10.06%) لدى الإناث، وهذا يؤكد دور متغيّر الجنس والتعرّض للخطورة.

أجرى الحكيم (2007م) دراسة وصفية لدور الضحية في حدوث الجريمة على ضحايا جرائم السرقات في مدينة الرياض، واستُخدم منهج المسح الاجتماعي بالعينة، وكشفت نتائج الدراسة أن لأنماط الشخصية والتصرفات السلوكية دورًا في وقوع بعض الضحايا فريسة لجريمة السرقة، وأظهرت نتائج الدراسة أنّ للخصائص الديموغرافية والاجتماعية والاقتصادية لضحايا جرائم السرقات دور في وقوعهم ضحية لجريمة السرقة، وأنّ لإهمال ضحايا السرقات في المحافظة على ممتلكاتهم دور في وقوعهم ضحية لجريمة السرقة.

أجرى هلال (2005م)، دراسة عن التحليل الاجتماعي لضحايا الجريمة، دراسة إحصائية لواقع الضحايا في إمارة الشارقة، وأسفرت النتائج على أنّ هناك العديد من الأضرار والآثار السلبية التي يعاني منها الضحايا من جراء تعرّضهم للجريمة، ومن أبرزها الأضرار النفسية والاجتماعية والاقتصادية. وكشفت نتائج التحليل الإحصائي للإحصاءات الجنائية الخاصة بإمارة الشارقة أنّ أكثر الجنسيات العربية التي يقع أبناؤها ضحايا للجريمة هي: الجنسية الإماراتية، والمصرية، والسورية، والأردنية والفلسطينية. وأنّ أكثر ضحايا الجريمة من الذكور، وبفارق كبير مقارنة بالإناث. كما كشفت النتائج على أنّ أغلب الضحايا يتراوح مستواهم التعليمي ما بين القراءة والكتابة والتعليم دون الجامعة.

أشار (المنشاوي، 2002م) في دراسته حول جرائم الإنترنت في المجتمع السعودي إلى أنّ ابتزاز المرأة لإيقاعها في الفاحشة تطوّر، واستخدمت فيه التقنية

لتهديدهـــا وإكراههـــا، وذلـــك بنـــشر صورهـــا عـــبر تقنيـــة الإنترنت بعـــد أن يتسـلّل الرجـل المبتـز إلى حاسـوب الفتـاة الشـخصي والاسـتيلاء عـلى الصـور الشـخصية لهـا، ثبـت مـن هـذه الدراسـة التطبيقيـة التـي تناولـت جرائـم الإنترنت في المجتمـع السـعودي أنّ (2.9%) قامـوا بإنشـاء مواقـع للتشـهير في آخريـن أو جعلـوا شـبكة الإنترنت متنفّسـًا لسـمومهم، ومكانـًا أمنـًا لارتـكاب أفعالهـم غـير الأخلاقيـة، كـما كشـفت الدراسـة أنّ معـدل (2.9%) مـن متصفّحـي الإنترنت ذكـروا بصراحـة أنهـم قـد تعرّضوا لضغـوط وابتـزاز وتشـهير مـن أجـل الإكـراه على ممارسـة أفعـال مشـينة.

التعليق على الدراسات السابقة:

اتّفقت دراسة (الشمري، 2011م) ودراسة (الحكيم، 2007م) على أنّ لأنماط الشخصية والتصرّفات السلوكية للضحايا دور في وقوع بعض الضحايا فريسة لجريمة.

اتّفقت دراسة (الحربي، 2011م) ودراسة (المطيري، 2008م) على أنّ تدنّي المستوى التعليمي للأفراد بشكلٍ عامٍّ يلعب دورًا في وقوعهم ضحايا الجريمة.

اتّفقت دراسة (هلال، 2012م) ودراسة (المطيري، 2008م) على الذين تتراوح أعمارهم ما بين (35-50) أكثر الفئات تعرّضًا للاحتيال، وهم متزوجون ومستواهم التعليمي منخفض.

واتّفقت دراسة (المنشاوي، 2002م) و(العنزي، 2016م) في استغلال وسائل التواصل الاجتماعي والإنترنت للإيقاع بالفتاة وابتزازها.

وقامت دراسة (الردايدة، 2006م) ودراسة (الزهراني، 2014م) على دراسة القانون وحمايته للضحايا.

فيما تتّفق الدراسة الحالية مع دراسة الحربي في استنادها على نظرية أسلوب الحياة في تفسيرها للضحايا، ومع دراسة (العموش، 2003م) في استخدام نظرية النوافذ المحطمة، ومن المتوقّع أن النتائج ستتوافق مع دراسة (الشمري، 2011م) ودراسة (الحكيم، 2007م) على أنّ لأنماط الشخصية والتصرّفات السلوكية للضحايا دور في وقوع بعض الضحايا فريسة لجريمة، ومن المتوقّع أنّ الدراسة ستتوافق مع نتائج دراسة (العموش، 2003م) و(هلال، 2005م) في أنّ للجنس علاقة حول الخبرة المباشرة للجريمة.

منهج الدراسة:

اعتمدت الدراسة على المنهج الكمي والكيفي من خلال تحليل ضحايا الاحتيال الإلكتروني في المجتمع الإماراتي.

عيّنة الدراسة:

تمّ توزيع الاستبيان على عيّنة من المقيمين والمواطنين تشكّلت من 2200 شخص بطريقة غرضية غير احتمالية من مجتمع الإمارات في الدوائر الحكومية والوزارات، حيث قمت بمسح اجتماعي لجميع الوزارات والدوائر الحكومية ولكن تم التوزيع في الجهات التي لم تمانع، وتم اعتماد عينة كرة الثلج في مجال وسائل التواصل الاجتماعي والأقارب للتعرف على الخبرة المباشرة للضحايا، الخبرة السابقة والخبرة المباشرة للأقارب ضحايا الاحتيال، وتم استخدام المقابلة مع عدد 42 من ضحايا الاحتيال الإلكتروني في الدوائر الحكومية أو أثناء التواصل طلبت مقابلتهم، وتم توزيع 2200 استبيان، والعائد منهم 1830 حيث تم حذف 300 استبيان لعدم اكتماله أو لعدم الصداقية

في الإجابة، و70 استبيان لم يتم استلامه، وتم توزيع الاستبيان كما يشار في الجدول الآتي:

المناطق التي تم توزيع الاستبيان فيها	العدد	المناطق التي تم توزيع الاستبيان فيها	العدد
إمارة عجمان	240	دبي	495
القيادة العامة لشرطة عجمان	60	النيابة العامة	30
محكمة عجمان	60	مرور دبي	70
هيئة الهوية للإمارات عجمان	30	القيادة العامة في شرطة دبي	190
اتصالات عجمان	25	دائرة الأراضي والأملاك	45
مصرف عجمان	30	وزارة الصحة	15
مركز شرطة الحميدية	35	وزارة العمل	35
الشارقة	560	وزارة تنمية المجتمع	25
مركز شرطة الغرب الشامل	30	مركز دبي للإحصاء	20
منطقة الشارقة التعليمية	35	الإدارة العامة للإقامة وشؤون الأجانب	60
محكمة الشارقة	40	دائرة الشؤون القانونية لحكومة دبي	5
محكمة الأسرة	40	أبوظبي	327
جامعة الشارقة	350 من إمارات مختلفة	وزارة تنمية المجتمع	60
البلدية ودائرة الأراضي والأملاك	25	هيئة التنمية الاقتصادية	120
مركز بحوث الشرطة	40	المجلس التنفيذي	40
أم القيوين	70	مؤسسة زايد العليا	20
القيادة العامة لشرطة أم القيوين	50	صندوق معاشات ومكافآت التقاعد لإمارة أبوظبي	40
غرفة التجارة والصناعة في أم القيوين	20	وزارة التغير المناخي والبيئة	7
رأس الخيمة	70	الأرشيف الوطني	60
غرفة التجارة والصناعة	30	الفجيرة	87

العدد	المناطق التي تم توزيع الاستبيان فيها	العدد	المناطق التي تم توزيع الاستبيان فيها
7	بلدية الفجيرة	30	وزارة الاقتصاد
200	الأقارب والأصدقاء من مختلف الإمارات	5	صندوق الشيخ خليفة
300	عن طريق السوشال ميديا من مختلف الإمارات	5	برنامج الشيخ صقر

أداة الدراسة:

تمّ تصميم استبانة يقوم أفراد المجتمع بتعبئتها، وقد تكوّنت في بدايتها قبل التحكيم من 5 مجالات، وهي: المعلومات الأساسية؛ وهي البيانات الأولية للمبحوثات وعباراتها (1-11)، ضحية الاحتيال الإلكتروني في الفترة السابقة بالنسبة للفرد شخصيًّا وبالنسبة لأقاربه، وعباراتها (11-22)، هل تخاف أن تتعرض للاحتيال الإلكتروني (23-34)، دور الضحية في تعرضها للاحتيال الإلكتروني (35-40)، من وجهة نظرك هل هذه العوامل تقلّل من الوقوع كضحايا للاحتيال الإلكتروني؟ (41-50) التعاون بين ضحايا الاحتيال الإلكتروني ورجال الأمن (51- 57).

صدق الآداة:

تم تحكيم الاستبيان من قبل 6 محكمين من الأساتذة والمتخصّصين من داخل الإمارات وخارجها، وتم إجراء التعديلات الآتية: المعلومات الأساسية؛ وهي البيانات الأوليه للمبحوثات وعباراتها (1-11) حذف الدخل الشهري الشخصي والاكتفاء بالدخل الشهري، وتم إضافة البيانات التقنية (11- 14) تم استبدال هل تخاف أن تتعرض للاحتيال الإلكتروني؟ بـــ هل تعلم بوجود أنواع الاحتيال الإلكتروني الشائعة في المجتمع؟ (15- 29)، وتم إضافة الاحتيال العاطفي والتسوّل الإلكتروني وانتحال صفة كبار الشخصيات، والاحتيال عبر الإعلان عن الوظائف الوهمية والاحتيال عن

طريق المحافظ الاستثمارية، تم تقسيم سؤال ضحية الاحتيال الإلكتروني في الفترة السابقة بالنسبة للفرد شخصيًّا، وبالنسبة لأقاربه إلى سؤالين: هل سبق أن تعرّضت للاحتيال الإلكتروني بإجابة (نعم، لا) (30– 45)، والسؤال الآخر: هل سبق أن تعرّض أحد أقاربك وأصدقائك للاحتيال الإلكتروني بإجابة (نعم، لا) (46–51). أمّا بند التعاون بين ضحايا الاحتيال الإلكتروني ورجال الأمن فتم تقسيمه إلى قسمين: القسم الأول في سؤالين: السؤال الأول قُمت بإبلاغ مَن عند التعرض للاحتيال؟ وسؤال آخر: إذا لم تبلّغ ما هي الأسباب؟ (52–54)، والقسم الآخر: القانون والضحايا (55–60)، دور الضحية في تعرّضها للاحتيال الإلكتروني (61–65)، التسوّق الإلكتروني (65–69)، وتم حذف بند من وجهة نظرك هل هذه العوامل تقلّل من الوقوع كضحايا للاحتيال الإلكتروني.

ثبات الآداة:

تمّ قياس ثبات الآداة بشكلٍ جزئي من خلال معامل ألفا كرونباخ، حيث إنه شكّل تساؤل هل أفراد العينة على دراية ووعي بأنواع الاحتيال الإلكتروني؟ معامل ثبات (0.836)، أمّا بالنسبة لتعرّض أفراد العيّنة للاحتيال معامل ثبات ألفا كرونباخ (0.940) تعرض أقارب أفراد العينة للاحتيال الإلكتروني (0.954)، أمّا القانون وضحايا الاحتيال (0.609)، أمّا دور الضحية في تعرّضها للاحتيال الإلكتروني (0.828).

الفصل الثاني
تحليل النتائج

الخصائص الديموجرافية والاجتماعية والاقتصادية لأفراد العينة:

الجدول رقم (1)

(يمثّل توزيع أفراد العيّنة حسب خصائص العينة الديموغرافية):

العمر	**التكرار**	**النسبة المئوية**	**محل الإقامة**	**التكرار**	**النسبة المئوية**
أقل من 18	63	3.4%	عجمان	198	10.8%
من 18- أقل من 30	915	50.0%	الشارقة	497	27.2%
من 30 إلى أقل من 40	516	28.2%	دبي	436	23.8%
من 40 إلى أقل من 50	256	14%	أبوظبي	407	22.2%
من 50 إلى أقل من 60	69	3.8%	أم القيوين	100	5.5%
60 سنة فأكثر	11	6%	رأس الخيمة	104	5.7%
المجموع	1830	100.0	الفجيرة	88	4.8%
الجنس	**التكرار**	**النسبة المئوية**	المجموع	1830	100.0
ذكر	761	41 %	**المستوى التعليمي**	**التكرار**	**النسبة المئوية**
أنثى	1069	58.4%	أمّيّ	5	0.3%
المجموع	1830	100.0%	يقرأ ويكتب	12	0.7%
الحالة الاجتماعية	**التكرار**	**النسبة المئوية**	ابتدائي	8	0.4%
أعزب	941	51.4%	إعدادي	38	%2.1

متزوج	824	45%	ثانوي	506	%27.7
مطلق	54	3.0%	بكالوريوس	1026	%56.1
أرمل	11	0.6%	دراسات عليا	235	12.8%
المجموع	1830	100.0	المجموع	1830	100.0

يبيّن الجدول رقم (1) توزيع أفراد العيّنة حسب المتغيّرات الديموغرافية، ويشير الجدول إلى أنّ أعلى فئة عمرية كانت في عمر 18 إلى أقل من 30 سنة بنسبة 50%، وتليها الفئة العمرية من 30 إلى أقل من 40 بنسبة 28.2%، وتليها الفئة العمرية من 40 إلى أقل من 50 بنسبة 14%، وتليها الفئة العمرية من 50 إلى أقل من 60 بنسبة 3.8%. وتليها الفئة العمرية التي أقل من 18 بنسبة 3.4%، وأخيرًا الفئة العمرية 60 سنة فأكثر بنسبة 0.6%. وأشار الجدول إلى ارتفاع أفراد العيّنة من الإناث بنسبة 58.4%، أمّا الذكور فقد شكّلوا نسبة 41.6% . وأشار الجدول إلى ارتفاع أفراد العيّنة العازبون بنسبة 51.4%، وتلتها فئة المتزوجون بنسبة 45%، وتلتها فئة المطلقون بنسبة 3.0، وأخيرًا الأرامل بنسبة 0.6%. وأظهر الجدول ارتفاع أفراد العينة المقيمين في إمارة الشارقة بنسبة 27.2%، تلتها إمارة دبي بنسبة 23.8%، وتلتها إمارة أبوظبي بنسبة 22.2% ثم إمارة عجمان بنسبة 10.8%، وتلتها إمارة رأس الخيمة بنسبة 5.7%، وتلتها إمارة أم القيوين، وكانت نسبتهم 5.5%، وجاءت أقلّ نسبة للفجيرة بنسبة 4.8%. ويشير الجدول إلى ارتفاع أفراد العينة في مستوى البكالوريوس بنسبة 56.1%، ويليه المستوى الثانوي بنسبة 27.7%، ويليه الدراسات العليا بنسبة 12.8% ثم المستوى الإعدادي 2.1% ثم يقرأ ويكتب بنسبة 0.7%، وبعد ذلك الابتدائي 0.4%، وأخيرًا أمّيّ 0.3%.

الجدول رقم (2)

(يتمحور حول خصائص العيّنة الاقتصادية):

الدخل الشهري للأسرة	التكرار	النسبة المئوية	مصدر الدخل	التكرار	النسبة المئوية
أقل من 10000	487	26.6%	عمل الأخت	4	.2%
من 10000 –أقل من 20000	505	27.6%	عمل الابنة	1	.1%
من 20000 –أقل من 30000	434	23.7%	عمل الزوجة	15	.8%
30000 فأكثر	404	22.1%	معاش تقاعد	77	4.2%
المجموع	1830	100.0	عمل	1445	79%
المسكن	**التكرار**	**النسبة المئوية**	الوالدين	78	4.3%
فيلا	974	54.6%	عقارات	14	.8%
بيت شعبي	403	22.6%	تجارة	57	3.1%
شقة	393	22.0%	الجمعيات الخيرية	9	.5%
أستوديو	9	.5%	عمل، تجارة، معاش تقاعد	7	.4%
سكن جامعي	6	.3%	عمل، معاش تقاعد	17	0.9%
المجموع	1830	100.0%	عمل، عمل الزوجة	16	.9%
المهنة	**التكرار**	**النسبة المئوية**	عمل، تجارة	73	4.0%
طالب	562	30.7%	المعونات الحكومية	17	0.9%
قطاع حكومي	883	48.3%			
قطاع خاص	117	6.4%	المجموع	1830	100.0
لا يعمل	123	6.7%			

أعمال حرة	38	2.1%			
قطاع شبه حكومي	107	5.8%			
المجموع	1830	100.0			

يبيّن الجدول (2) ارتفاع أفراد العيّنة بمهن القطاع الحكومي بنسبة 48.3%، تليها طالب 30.7%، لا يعمل بنسبة 6.4% ثم القطاع الخاص بنسبة 6.4% ثم القطاع شبه الحكومي بنسبة 5.8%، وأخيرًا الأعمال الحرة بنسبة 2.1%.
يبيّن الجدول ارتفاع أفراد العينة الذين دخلهم من 10000 -أقل من 20000 بنسبة 27.6%، ويليه أفراد العيّنة الذين دخلهم أقل من 10000 بنسبة 26.6%، ويلية أفراد العينة الذين دخلهم من20000 – أقل من30000 بنسبة 23.7%، وأخيراً 30000 فأكثر بنسبة 22.1%. ويبيّن الجدول ارتفاع أفراد العينة الذين مصدر دخلهم من خلال العمل بنسبة 79%، ومن الوالدين 4.3%، ومن معاشال تقاعد 4.2%، (العمل، التجارة) 4%، التجارة بنسبة 3.1%، واشترك الذين مصدر دخلهم (عمل ومعاش تقاعد) والمعونات الحكومية و(عمل وعمل الزوجة) نسبة 0.9%، اشترك الذين مصدر دخلهم عقارات مع عمل الزوجة بنسبة 0.8%، من الجمعيات الخيرية 0.5%، يليه الذين مصدر دخلهم من (عمل، تجارة، معاش تقاعد) 0.4%، ثم عمل الأخت 0.2%، وأخيرًا عمل الابنة 0.1%. وأظهر الجدول ارتفاع أفراد العيّنة الذين يسكنون في فيلا بنسبة 54.8%، ثم الذين يسكنون في بيت شعبي 22.3%، ثم في شقة بنسبة 22%، وأستوديو 0.5%، وأخيرًا في سكن جامعي 0.3%.

الجدول (3)

(يتمحور حول توزيع أفراد العينة بحسب الجنسية):

الجنسية	التكرار	النسبة المئوية	الجنسية	التكرار	النسبة المئوية
إماراتي	1280	69.9%	كندا	2	0.1%
دول مجلس التعاون	118	6.4%	السودان	30	1.6%

الجنسية	التكرار	النسبة المئوية	الجنسية	التكرار	النسبة المئوية
مصر	66	3.6%	جزر القمر	19	1.0%
فلسطين	23	1.3%	الهند	12	0.7%
اليمن	26	1.4%	باكستان	4	0.2%
الأردن	48	2.6%	فرنسا	1	0.1%
سوريا	61	3.3%	أمريكا	3	0.2%
لبنان	7	0.4%	تونس	3	0.2%
إيران	12	.7%	بريطانيا	1	0.1%
الجزائر	4	.2%	الصومال	3	0.2%
العراق	25	1.4%	إثيوبيا	3	0.2%
جنسيات عربية غير محددة	78	4.3%	موريتانيا	1	0.1%
المجموع	1830	100.0	المجموع	1830	100.0

يشير الجدول (3) إلى توزيع أفراد العينة حسب الجنسية فكانت كالآتي: حيث ارتفعت نسبة أفراد العينة من الجنسية الإماراتية بنسبة 69.9% تلتها دول مجلس التعاون 6.4% بعد ذلك الجنسيات الآتية والمرتبة كالآتي: مصر بنسبة 3.6% ثم سوريا بنسبة 3.3 % ثم الأردن بنسبة 2.6%، السودان 1.6%، اليمن 1.4%، العراق 1.4%، فلسطين 1.3%، جزر القمر1%، إيران والهند 0.7%، لبنان 0.4%، أمّا الجزائر، أمريكا، تونس، إثيوبيا، الصومال، باكستان 0.2% أمّا موريتانيا، كندا، فرنسا، بريطانيا فشكّلوا 0.1%، وأخيرًا الجنسيات العربية الأخرى التي رفض أفراد العينة التصريح بها واكتفوا بقول أنا عربي فكانت 4.3%.

البيانات التقنية الأساسية:

الجدول رقم (4)

الهواتف الذكية

أنواع الهواتف التي تستخدمها	الهواتف الذكية	الهواتف التقليدية	المجموع
التكرارات	1812	18	1830
النسبة المئوية	99.0	1.0	100

المدة الزمنية التي تقضيها في استخدام الهواتف الجوالة	أقل من ساعة	من ساعة إلى أقل من ساعتين	من ساعتين إلى أقل من 3 ساعات	3 ساعات فأكثر	المجموع
التكرارات	167	332	401	930	1830
النسبة المئوية	9.1	18.1	21.9	50.8	100

يشير الجدول رقم (4) إلى أنواع الهواتف التي تستخدمها أفراد العينة، فيلاحظ ارتفاع نسبة استخدام الهواتف الذكية بنسبة 99%، أمّا الهواتف التقليدية فشكّلت 1% فقط من أفراد العينة، وذلك بسبب التطور التقني وأن الهواتف الحديثة أصبحت أحد متطلبات العصر.

يبيّن الجدول ارتفاع أفراد العينة الذين يزيد مدة استخدامهم للهواتف عن 3 ساعات ووصلت نسبتهم إلى 50.8% يليه من ساعتين إلى أقل من 3 ساعات بنسبة 21.9% يليه من ساعة إلى أقل من ساعتين بنسبة 18.1%، وأخيرًا أقل من ساعة بنسبة 9.1%، وهذا يدلّ على زيادة استخدام الهواتف الذي من شأنه أن يجعل الأفراد يتعرّفون على العديد من الناس من خلال الهواتف، الأمر الذي ربما يؤدّي إلى وقوعهم كضحايا للاحتيال الإلكتروني.

الجدول رقم (5)

وسائل التواصل الاجتماعي:

وسائل التواصل الاجتماعي المستخدمة	لا شيء	Twitter	facebook	snapchat	instagram	whatsapp	telegram	email	LinkedIn	YouTube	جميع وسائل التواصل الاجتماعي
التكرارات	29	47	68	100	140	61	3	1	1	6	1374
النسبة المئوية	1.6%	2.6%	3.7%	5.5%	7.7%	3.3%	.2%	.1%	.1%	.3%	75.1%

المدة الزمنية التي تقضيها في استخدام وسائل التواصل الاجتماعي	أقل من ساعة	من ساعة إلى أقل من ساعتين	من ساعتين إلى أقل من 3 ساعات	3 ساعات فأكثر	لا أستخدمها نهائيًا	المجموع
التكرارات	249	465	415	664	37	1830
النسبة المئوية	13.6	25.4	22.7	36.3	2.0	100

يشير الجدول (5) إلى أنّ معظم أفراد العينة يستخدمون جميع وسائل التواصل الاجتماعي، وشكّلت نسبتهم 75.1%، يليه الذين يستخدمون الأنستجرام بنسبة 7.7%، يليه الذين يستخدمون السناب شات 5.5%، ثم الذين يستخدمون الفيس بوك بنسبة 3.7%، يليه الذين يستخدمون الواتس آب 3.3%، ثم الذين يستخدمون تويتر بنسبة 2.6%، ويليه الذين لا يستخدمون وسائل التواصل الاجتماعي بنسبة 1.6%، يليه

الذين يستخدمون اليوتيوب بنسبة 0.3%، يليه الذين يستخدمون التليغرام 0.2%، وأخيرًا الذين يستخدمون الإيميل واللينكدين 0.1%.

<table dir="rtl">
<tr><th colspan="3">الدفع عند الاستلام</th><th colspan="3">الدفع المسبق عن طريق بطاقة الدفع الإلكتروني</th></tr>
<tr><th>التكرارات</th><th colspan="2">النسبة المئوية</th><th>التكرارات</th><th colspan="2">النسبة المئوية</th></tr>
<tr><td>1187</td><td colspan="2">79.8</td><td>309</td><td colspan="2">20.2</td></tr>
<tr><th>هل بسبب</th><th>التكرارات</th><th>النسبة المئوية</th><th>هل بسبب</th><th>التكرارات</th><th>النسبة المئوية</th></tr>
<tr><td>خوفًا من عدم وصول البضاعة</td><td>171</td><td>11.49</td><td>سهولة إنجاز المعاملة</td><td>173</td><td>11.31</td></tr>
<tr><td>خوفًا من عدم مطابقة البضاعة للمواصفات</td><td>94</td><td>6.31</td><td>الخصم الذي يعطى على البطاقة في حال الدفع قبل الاستلام</td><td>39</td><td>2.55</td></tr>
<tr><td>خوفًا من سرقة بطاقة الائتمان</td><td>28</td><td>1.88</td><td>الثقة الزائدة</td><td>16</td><td>1.05</td></tr>
<tr><td>كلّ ما سبق</td><td>886</td><td>59.56</td><td>سياسة الشركة</td><td>9</td><td>.59</td></tr>
<tr><td rowspan="3">المجموع</td><td rowspan="3">1179</td><td rowspan="3">79.8</td><td>عدم استخدامي للمبالغ النقدية</td><td>2</td><td>.131</td></tr>
<tr><td>كل ما سبق</td><td>90</td><td>5.88</td></tr>
<tr><td>المجموع</td><td>329</td><td>20.2</td></tr>
</table>

ارتفاع أفراد العيّنة الذين يزيد مدة استخدامهم وسائل التواصل الاجتماعي عن 3 ساعات ووصلت نسبتهم إلى 36.3%، يليه من ساعة إلى أقل من ساعتين بنسبة 25.4%، ثم من ساعتين إلى أقل من 3 ساعات بنسبة 22.7%، ويليه أقل من ساعة بنسبة 13.6% وأخيرًا الذين لا يستخدمونها نهائيًا 2.0%.

الجدول رقم (6)

التسوّق الإلكتروني

هل تتسوّق إلكترونيًّا	التكرارات	النسبة المئوية
نعم	1487	81.3
لا	343	18.7
المجموع	1830	100.0

يشير الجدول إلى أنّ عدد الذين يتسوقون إلكترونيًّا بلغت نسبتهم 81.3 %، أمّا الذين لا يتسوقون إلكترونيًّا فبلغ 18.7%، وربما النسبة عالية بسبب طرح السؤال بشكل عام.

يشير الجدول إلى أنّ 1487 من أفراد العينة يتسوّقون إلكترونيًّا، وانقسم إلى أن الذين يفضّلون وسيلة الدفع عند الاستلام عند التسوق إلكترونيًّا بلغت نسبتهم 79.8 من الذين يتسوّقون إلكترونيًّا للأسباب الآتية: خوفًا من عدم وصول البضاعة بنسبة 11.49%، خوفًا من عدم مطابقة البضاعة للمواصفات بنسبة 6.31%، خوفًا من سرقة بطاقة الائتمان بنسبة 1.88%، أمّا كلّ ما سبق 59.56%، أمّا الذين يفضلون وسيلة الدفع المسبق عن طريق بطاقة الدفع الإلكتروني عند التسوق إلكترونيًّا فبلغت نسبتهم 20.2% من الذين يتسوّقون إلكترونيًّا للأسباب الآتية: سهولة إنجاز المعاملة بنسبة 11.31%، الخصم الذي يعطى على البطاقة في حال الدفع قبل الاستلام 2.55%، الثقة الزائدة 1.05%، سياسة الشركة 0.59%، عدم استخدامه للمبالغ النقدية 0.131%، وأخيرًا جميع ما سبق 5.88%.

ويلاحظ ارتفاع عدد الذين يفضّلون الدفع عند الاستلام أكثر من الدفع المسبق لما له من دور في زيادة جرائم الاحتيال عبر التسوق التجاري وسرقة بيانات البطاقة والاستيلاء على أموال الضحية من خلالها.

هل لاستخدام برامج التواصل الاجتماعي والتسوق الإلكتروني دور في التعرض للاحتيال الإلكتروني؟

الجدول (7)

يتمحور حول دور برامج التواصل الاجتماعي في التعرض للاحتيال الإلكتروني

هل سبق أن تعرضت لأحد صور الاحتيال الإلكتروني التي سبق ذكرها	وسائل التواصل الاجتماعي المستخدمة											
	لا شيء	twitter	facebook	snapchat	instagram	whatsapp	telegram	linkdin	Email	Youtube	جميع وسائل التواصل الاجتماعي	المجموع
نعم	3	14	35	23	50	16	0	0	0	1	422	564
لا	26	33	33	77	90	45	3	1	1	5	952	1266
المجموع	29	47	68	100	140	61	3	1	1	6	1374	1830

يظهر الجدول (7) أنّ عدد الذين لا يستخدمون وسائل التواصل الاجتماعي بلغ 29 منهم 3 تعرضوا للاحتيال و26 لم يتعرضوا، وعدد الذين يستخدمون التويتر بلغ عددهم 47 منهم 14 تعرضوا للاحتيال و33 لم يتعرضوا للاحتيال، وأشار الجدول إلى أنّ عدد الذين يستخدمون الفيس بوك بلغ عددهم 68 منهم 35 تعرضوا للاحتيال و33 لم يتعرضوا للاحتيال، وبالنسبة إلى عدد الذين يستخدمون السناب شات بلغ عددهم 100 منهم 23 تعرضوا للاحتيال و77 لم يتعرضوا للاحتيال، أمّا عدد الذين يستخدمون الأنستجرام فبلغ عددهم 140 منهم 50 تعرضوا للاحتيال و90 لم يتعرضوا للاحتيال، وأشار الجدول إلى أنّ عدد الذين يستخدمون الواتساب بلغ عددهم 61 منهم 16 تعرضوا للاحتيال و45 لم يتعرضوا للاحتيال، أمّا بالنسبة إلى عدد الذين يستخدمون التليغرام فبلغ عددهم 3 لم يتعرضوا للاحتيال، أمّا عدد الذين يستخدمون اليوتيوب فبلغ عددهم 6، منهم 1 تعرضوا للاحتيال و5 لم يتعرضوا للاحتيال، أمّا عدد الذين يستخدمون النك دين فبلغ 1 لم يتعرض للاحتيال، والذين يستخدمون الإيميل 1

لم يتعرض للاحتيال، وأخيرًا أشار الجدول إلى أنه بلغ عدد الذين يستخدمون جميع وسائل التواصل الاجتماعي 1372 منهم 421 تعرضوا للاحتيال و951 لم يتعرضوا للاحتيال.

يشير الجدول إلى وجود علاقة ضعيفة ذات دلالة إحصائية بين التعرض للاحتيال الإلكتروني وبين وسائل التواصل الاجتماعي المستخدمة (a=0.002 , cc:0.121)

الجدول رقم (8)

هل لاستخدام التسوق الإلكتروني دور في التعرض للاحتيال الإلكتروني؟

هل تتسوّق إلكترونيًّا	هل سبق أن تعرضت لأحد صور الاحتيال الإلكتروني			
	نعم	لا	المجموع	الدلالة الإحصائية
نعم	494	993	1487	Contingency Coefficient :0.000
لا	70	273	343	
المجموع	564	1266	1830	

يشير الجدول (8) إلى أنّ عدد الذين يتسوقون إلكترونيًّا بلغ 1478 منهم 494 ضحية تعرضوا للاحتيال الإلكتروني، أمّا عدد الذين لا يتسوقون إلكترونيًّا فبلغ 343 منهم 70.

ويشير الجدول إلى وجود علاقة ذات دلالة إحصائية بين التسوّق الإلكتروني والتعرض للاحتيال الإلكتروني. (cc:000)

الجدول رقم (9)

الوعي بأنواع الاحتيال الإلكتروني

ما صور الاحتيال الإلكتروني الشائعة في المجتمع؟	موجود		لا أعلم		غير موجود	
	التكرار	النسبة المئوية	التكرار	النسبة المئوية	التكرار	النسبة المئوية
الاحتيال والنصب عبر الهاتف	1716	93.8	81	4.4	33	1.8

الاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي	1623	88.7	161	8.8	46	2.5
الاحتيال الإلكتروني العاطفي	1573	86.0	205	11.2	52	2.8
التسوّل الإلكتروني	1559	85.2	196	10.7	75	4.1
الاحتيال الإلكتروني التجاري	1526	83.4	235	12.8	69	3.8
الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان	1500	82.0	249	13.6	81	4.4
انتحال صفة كبار الشخصيات	1464	80.0	298	16.3	68	3.7
الاحتيال عن طريق الإعلان عن الوظائف الوهمية	1393	76.1	343	18.7	94	5.1
الاحتيال عن طريق المحافظ الاستثمارية الوهمية الإلكترونية	1223	66.8	527	28.8	80	4.4
الاحتيال الإلكتروني عن طريق اليانصيب	1147	62.7	546	29.8	137	7.5
الاحتيال الإلكتروني عن طريق الشركات	1125	61.5	596	32.6	109	6
تزوير بطاقة الائتمان	1058	57.8	599	32.7	173	9.5
الاحتيال الإلكتروني عن طريق موظّفي المصارف	1021	55.8	633	34.6	176	9.6
سوق العملة الإلكتروني (بيع العملة الافتراضية)	973	53.2	747	40.8	110	6.0

هل أفراد العينة على دراية ووعي بأنواع الاحتيال الإلكتروني؟

يشير الجدول (9) إلى وعي أفراد العينة وإدراكهم لأنماط الاحتيال الإلكتروني وصوره الشائعة بالمجتمع الإماراتي، فيتّضح من الجدول أنّ معظم أفراد العينة يعرفون بوجود أنواع الاحتيال الإلكتروني، ويشير الجدول إلى أن أعلى نسبة هي: الاحتيال والنصب عبر الهاتف، فقد شكّلت نسبة الذين أجابوا بأنه موجود 93.8%، والذين لا يعلمون 4.4%، أمّا الذين أجابوا بغير موجود فكانوا 1.8%، وسبب ارتفاع المعرفة بهذا النوع من الاحتيال يعود لانتشاره، فلا يوجد شخص لم تصله رسائل هاتفية تفيد بأنه ربح مبالغ مالية أو جوائز قيمة، وهناك الكثير من الناس الذين يصدقونهم ويقومون بتحويل مبالغ لهم، يليه الاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي، حيث شكّلت نسبة الذين أجابوا بأنه موجود 88.7%، أمّا الذين لا يعلمون بوجوده 8.8%، و2.5% قالوا بأنه غير موجود، ويعود ارتفاع الوعي إلى زيادة اختراق وسائل التواصل الاجتماعي وطلب المال من أصدقاء الضحية، ويليه الاحتيال الإلكتروني العاطفي، حيث شكّلت نسبة الذين أجابوا بأنه موجود 86% أمّا الذين لا يعلمون بوجوده 11.2%، وغير الموجود 2.8%، فانتشرت العلاقات العاطفية من خلال الإنترنت، ويتم ذلك عندما يبني المحتال علاقة قوية على الإنترنت مع شخص ما، ويتم إقناع الضحية بإرسال صورة أو أيّ بيانات أخرى للمحتال، ويقوم المحتال بطلب أموال لعدم نشر المحتوى، يليه التسوّل الإلكتروني حيث شكّلت نسبة الذين أجابوا بأنه موجود 85.2% أمّا لا أعلم فبنسبة 10.7%، وغير الموجود 4.1%، وذلك بادعاء أشخاص للفقر عن طريق وسائل التواصل الاجتماعي وهم ليسوا فقراء، يليه الاحتيال الإلكتروني التجاري، وذلك من خلال التسوق الإلكتروني حيث شكّلت نسبة الذين أجابوا بأنه موجود 83.4% أمّا لا أعلم 12.8%، وغير موجود 3.8%، ويتم عند عدم وصول البضاعة أو وصول بضاعة آخرى، يليه الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان، فشكّلت نسبة الذين أجابوا بأنه موجود 82.0%، لا أعلم 13.6%، وغير موجود 4.4%، يليه انتحال صفة كبار الشخصيات فشكّلت نسبة الذين أجابوا بأنه موجود 80.0%، لا أعلم 16.3%، وغير موجود 3.7%، ما انتشر بالفترة

الماضية عن طريق وسائل التواصل الاجتماعي بانتحال بعض الشخصيات لصفة شيوخ وطلب تحويل أموال لهم، يليه الاحتيال عن طريق الإعلان عن الوظائف الوهمية فشكّلت نسبة الذين أجابوا بأنه موجود 76.1%، لا أعلم 18.7%، وغير موجود 5.1%، يليه الاحتيال عن طريق المحافظ الاستثمارية الوهمية الإلكترونية حيث شكّلت نسبة الذين أجابوا بأنه موجود 66.8%، لا أعلم 28.8%، وغير موجود 4.4%، يليه الاحتيال الإلكتروني عن طريق اليانصيب فشكلت نسبة الذين أجابوا بأنه موجود 62.7%، لا أعلم 29.8%، وغير موجود 7.5%، يليه الاحتيال الإلكتروني عن طريق الشركات فشكّلت نسبة الذين أجابوا بأنه موجود 61.5%، لا أعلم 32.6%، وغير موجود 6.0%، يليه تزوير بطاقة الائتمان فشكّلت نسبة الذين أجابوا بأنه موجود 57.8%، لا أعلم 32.7%، وغير موجود 9.5%، يليه الاحتيال الإلكتروني عن طريق موظّفي المصارف شكّلت نسبة الذين أجابوا بأنه موجود 55.8%، لا أعلم 34.6%، وغير موجود 9.6%، وأخيرًا الاحتيال عن طريق سوق العملة الإلكتروني (بيع العملة الافتراضية) شكّلت نسبة الذين أجابوا بأنه موجود 53.2%، لا أعلم 40.6%، وغير موجود 6.0%.

هل سبق أن تعرضت لأحد صور الاحتيال الإلكتروني	نعم	لا	المجموع
النسبة المئوية	30.8	69.2	100
التكرارات	564	1266	1830

أنماط الاحتيال الإلكتروني التي سبق وتعرّض لها أفراد العينة موزّعة في الجدول (10) على حسب أعداد الضحايا والجرائم التي تعرضوا لها: يمثل أعداد الضحايا 564 ضحية، ولكن العدد الكبير يعود إلى أن معظم الضحايا قد تعرضوا لأكثر من نوع من أنواع الاحتيال الإلكتروني.

أنماط الاحتيال الإلكتروني التي سبق وتعرّض لها أفراد العينة موزّعة في الجدول (10) على حسب أعداد الضحايا والجرائم التي تعرضوا لها.

الجدول (10)

أنماط الاحتيال الإلكتروني التي سبق وتعرّض لها أفراد العينة:

أنواع الاحتيال الإلكتروني التي تعرض لها أفراد العينة	منذ أقل من 12 شهر	منذ سنتين	منذ أكثر من 3 سنوات	المجموع	
				التكرار	النسبة المئوية
الاحتيال والنصب عبر الهاتف	171	56	36	263	46.63
الاحتيال الإلكتروني التجاري وذلك من خلال التسوق الإلكتروني	120	52	40	212	37.59
الاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي	121	49	23	193	34.22
التسوّل الإلكتروني	120	29	20	169	29.96
انتحال صفة كبار الشخصيات	117	25	16	158	28.00
الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان	58	31	33	122	21.63
الاحتيال الإلكتروني العاطفي	73	22	26	121	21.45
الاحتيال الإلكتروني عن طريق الشركات	56	37	24	117	20.74
سوق العملة الإلكتروني (بيع العملة الافتراضية)	55	32	27	114	20.21
الاحتيال عن طريق المحافظ الاستثمارية الوهمية الإلكترونية	57	21	23	101	17.91
الاحتيال الإلكتروني عن طريق موظّفي المصارف	52	26	23	101	17.91

17.2	97	13	21	63	الاحتيال عن طريق الإعلان عن الوظائف الوهمية
17.2	97	18	19	60	الاحتيال الإلكتروني عن طريق اليانصيب
17.2	51	17	18	16	تزوير بطاقة الائتمان

يشير الجدول (10) إلى التوافق التقريبي بين إدراك ومعرفة أفراد العينة بأنواع الاحتيال الإلكتروني وتعرضهم لها، فيؤكد هذا السؤال على أن للجهل بأساليب الاحتيال دور في تعرض الضحية للاحتيال الإلكتروني فنتيجة لجهلهم في السابق تعرضوا للاحتيال الإلكتروني، وجاءت المعرفة بالاحتيال بعد التعرض له أو بعد تعرض أحد الأقارب، فيشير الجدول إلى ارتفاع ضحايا الاحتيال والنصب عبر الهاتف، فقد وصل عدد الضحايا 263 ضحية بنسبة 46.63% من مجموع أعداد الضحايا انقسموا إلى 171 ضحية تعرضوا للاحتيال والنصب عبر الهاتف منذ أقل من 12 شهر، و56 ضحية منذ سنتين و36 ضحية منذ 3 سنوات وتوافق مع إدراك أفراد العينة، حيث كانت أعلى نسبة الاحتيال والنصب عبر الهاتف، فقد شكّلت نسبة الذين أجابوا بأنه موجود 93.8%، الاحتيال والنصب عبر الهاتف فقد شكلت نسبة الذين أجابوا بأنه موجود 93.8%، بعدد 1716 من إجمالي أفراد العينة، فالكثير قد تعرّضوا لعصابات النصب والعديد من الأفراد يصدقونهم نتيجة الجهل، يليه الاحتيال الإلكتروني التجاري وذلك من خلال التسوق الإلكتروني وصل عدد الضحايا 212 ضحية بنسبة 37.59% من مجموع أعداد الضحايا انقسموا إلى 120 ضحية تعرضوا للاحتيال الإلكتروني التجاري، وذلك من خلال التسوق الإلكتروني منذ أقل من 12 شهر و52 ضحية منذ سنتين و40 ضحية منذ 3 سنوات، يليه الاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي، حيث وصل عدد الضحايا 193 ضحية بنسبة 34.22% من مجموع أعداد الضحايا انقسموا إلى 121 ضحية تعرضوا للاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي منذ أقل من 12 شهر و49 ضحية منذ سنتين و23 ضحية منذ 3 سنوات،

يليه التسوّل الإلكتروني حيث وصل عدد الضحايا 169 ضحية بنسبة 29.96% انقسموا إلى 120 ضحية تعرضوا للتسول الإلكتروني منذ أقل من 12 شهر و29 ضحية منذ سنتين و20 ضحية منذ 3 سنوات، يليه انتحال صفة كبار الشخصيات حيث وصل عدد الضحايا 158 ضحية بنسبة 28.0% انقسموا إلى 117 ضحية تعرضوا للاحتيال عن طريق انتحال صفة كبار الشخصيات منذ أقل من 12 شهر و25 ضحية منذ سنتين و16 ضحية منذ 3 سنوات، يليه الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان حيث وصل عدد الضحايا 122 ضحية بنسبة 21.61% انقسموا إلى 58 ضحية تعرضوا للاحتيال عن طريق، الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان منذ أقل من 12 شهر و31 ضحية منذ سنتين و33 ضحية منذ 3 سنوات، يليه الاحتيال الإلكتروني العاطفي حيث وصل عدد الضحايا 121 ضحية بنسبة 21.45% انقسموا إلى 73 ضحية تعرضوا للاحتيال الإلكتروني العاطفي منذ أقل من 12 شهر و22 ضحية منذ سنتين و26 ضحية منذ 3 سنوات، يليه الاحتيال الإلكتروني عن طريق الشركات.

حيث وصل عدد الضحايا 117 ضحية بنسبة 20.74% انقسموا إلى 56 ضحية تعرضوا للاحتيال عن طريق الشركات منذ أقل من 12 شهر و37 ضحية منذ سنتين و24 ضحية منذ 3 سنوات، يليه سوق العملة الإلكتروني (بيع العملة الافتراضية) وتعارض مع وعي أفراد العينة، حيث كان في المرحلة الأخيرة، فهذا من شأنه أن يؤدي إلى زيادة ضحايا العملة الافتراضية نتيجة للجهل من قبل أفراد العينة ووصل عدد الضحايا 114 ضحية بنسبة 20.21% انقسموا إلى 55 ضحية تعرضوا للاحتيال سوق العملة الإلكتروني (بيع العملة الافتراضية) منذ أقل من 12 شهر و32 ضحية منذ سنتين و27 ضحية منذ 3 سنوات يليه الاحتيال عن طريق المحافظ الاستثمارية الوهمية الإلكترونية حيث وصل عدد الضحايا 101 ضحية بنسبة 17.91% انقسموا إلى 57 ضحية تعرضوا للاحتيال عن طريق المحافظ الاستثمارية الوهمية الإلكترونية

منذ أقل من 12 شهر و21 ضحية منذ سنتين و23 ضحية منذ 3 سنوات يليه، الاحتيال الإلكتروني عن طريق موظفي المصارف وصل عدد الضحايا 101 ضحية بنسبة 17.91% انقسموا إلى 52 ضحية تعرضوا للاحتيال الإلكتروني عن طريق موظفي المصارف منذ أقل من 12 شهر و26 ضحية منذ سنتين و23 ضحية منذ 3 سنوات، يليه الاحتيال الإلكتروني عن طريق اليانصيب حيث وصل عدد الضحايا 97 ضحية بنسبة 17.2% انقسموا إلى 60 ضحية تعرضوا للاحتيال الإلكتروني عن طريق اليانصيب منذ أقل من 12 شهر و19 ضحية منذ سنتين و18 ضحية منذ 3 سنوات، يليه الاحتيال عن طريق الإعلان عن الوظائف الوهمية حيث وصل عدد الضحايا إلى 97 ضحية بنسبة 17.2% انقسموا إلى 63 ضحية تعرضوا للاحتيال عن طريق الإعلان عن الوظائف الوهمية منذ أقل من 12 شهر و21 ضحية منذ سنتين و13 ضحية منذ 3 سنوات، يليه تزوير بطاقة الائتمان حيث وصل عدد الضحايا 51 ضحية بنسبة 9.04% انقسموا إلى 16 ضحية تعرضوا للاحتيال عن طريق تزوير بطاقة الائتمان منذ أقل من 12 شهر و18 ضحية منذ سنتين و17 ضحية منذ 3 سنوات.

هل سبق أن تعرّض أحد أقاربك أو أصدقائك لأحد صور الاحتيال الإلكتروني	نعم	لا	المجموع
النسبة المئوية	44.8	55.2	100
التكرارات	819	1011	1830

الجدول رقم (11)

يبيّن تعرّض أقارب وأصدقاء أفراد العينة للاحتيال الإلكتروني

أنواع الاحتيال الإلكتروني التي تعرّض لها أقارب أفراد العينة	منذ أقل من 12 شهر	منذ سنتين	منذ أكثر من 3 سنوات	المجموع	
				التكرار	النسبة المئوية
الاحتيال والنصب عبر الهاتف	246	70	52	368	44.93

أنواع الاحتيال الإلكتروني التي تعرّض لها أقارب أفراد العينة	منذ أقل من 12 شهر	منذ سنتين	منذ أكثر من 3 سنوات	المجموع	
				التكرار	النسبة المئوية
الاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي	196	56	35	287	35.04
الاحتيال الإلكتروني التجاري	162	67	37	266	32.47
الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان	112	73	51	236	28.82
الاحتيال الإلكتروني العاطفي	122	62	38	222	27.11
انتحال صفة كبار الشخصيات	127	50	23	200	24.42
التسوّل الإلكتروني	124	44	27	195	23.81
الاحتيال عن طريق المحافظ الاستثمارية الوهمية الإلكترونية	78	46	53	177	21.61
الاحتيال الإلكتروني عن طريق الشركات	93	47	34	174	21.25
سوق العملة الإلكتروني (بيع العملة الافتراضية)	96	47	24	167	20.39
الاحتيال الإلكتروني عن طريق موظّفي المصارف	77	43	39	159	19.41
الاحتيال عن طريق الإعلان عن الوظائف الوهمية	89	47	19	155	18.93
الاحتيال الإلكتروني عن طريق اليانصيب	80	41	33	154	18.80
تزوير بطاقة الائتمان	45	29	26	100	12.21

تمّ الوصول إلى 819 ضحية من أقارب وأصدقاء العينة بنسبة 44.8% من أفراد العينة وموزعة كما موضح في الجدول أدناه

أنماط الاحتيال الإلكتروني التي سبق وتعرض لها أقارب وأصدقاء أفراد العينة موزعة في الجدول (12) على حسب أعداد الضحايا والجرائم التي تعرضوا لها.

يشير الجدول إلى ارتفاع أقارب أفراد العينة من ضحايا الاحتيال والنصب عبر الهاتف، فقد وصل عدد الضحايا 368 ضحية بنسبة 44.93% انقسموا إلى 246 ضحية تعرضوا للاحتيال والنصب عبر الهاتف منذ أقل من 12 شهر و70 ضحية منذ سنتين و52 ضحية منذ 3 سنوات، وتوافق مع إدراك أفراد العينة حيث كانت أعلى نسبة الاحتيال والنصب عبر الهاتف، فقد شكّلت نسبة الذين أجابوا بأنه موجود 93.8 بعدد 1716 من إجمالي أفراد العينة، فالكثير قد تعرضوا لعصابات النصب والعديد من الأفراد يصدقونهم نتيجة الجهل، يليه الاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي حيث وصل عدد الضحايا 287 ضحية بنسبة 35.04% انقسموا إلى 196 ضحية تعرضوا للاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي منذ أقل من 12 شهر و56 ضحية منذ سنتين و35 ضحية منذ 3 سنوات، يليه الاحتيال الإلكتروني التجاري وذلك من خلال التسوق الإلكتروني وصل عدد الضحايا 266 ضحية بنسبة 32.47% انقسموا إلى 162 ضحية تعرضوا للاحتيال الإلكتروني التجاري، وذلك من خلال التسوق الإلكتروني منذ أقل من 12 شهر و67 ضحية منذ سنتين و37 ضحية منذ 3 سنوات، يليه الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان حيث وصل عدد الضحايا 236 ضحية بنسبة 28.82% انقسموا إلى112 ضحية تعرضوا للاحتيال عن طريق الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان منذ أقل من 12 شهر و73 ضحية منذ سنتين و51 ضحية منذ 3 سنوات، يليه الاحتيال الإلكتروني العاطفي حيث وصل عدد الضحايا 222 ضحية بنسبة 27.11% انقسموا إلى 122 ضحية تعرضوا للاحتيال الإلكتروني العاطفي منذ أقل من 12 شهر و62 ضحية منذ سنتين و38 ضحية منذ 3 سنوات، يليه انتحال صفة كبار الشخصيات حيث وصل عدد الضحايا 200 ضحية بنسبة 24.42% انقسموا إلى 127 ضحية تعرّضوا للاحتيال عن طريق انتحال صفة كبار الشخصيات منذ أقل من

12 شهر، و50 ضحية منذ سنتين، و23 ضحية منذ 3 سنوات، يليه التسول الإلكتروني حيث وصل عدد الضحايا 195 ضحية بنسبة 23.81% انقسموا إلى 124 ضحية تعرضوا للتسول الإلكتروني منذ أقل من 12 شهر و44 ضحية منذ سنتين و27 ضحية منذ 3 سنوات، يليه الاحتيال عن طريق المحافظ الاستثمارية الوهمية الإلكترونية حيث وصل عدد الضحايا 177 ضحية بنسبة 21.61% انقسموا إلى 78 ضحية تعرضوا للاحتيال عن طريق المحافظ الاستثمارية الوهمية الإلكترونية منذ أقل من 12 شهر، و46 ضحية منذ سنتين و53 ضحية منذ 3 سنوات، يليه الاحتيال الإلكتروني عن طريق الشركات حيث وصل عدد الضحايا 174 ضحية بنسبة 21.25% انقسموا إلى 93 ضحية تعرضوا للاحتيال عن طريق الشركات منذ أقل من 12 شهر، و47 ضحية منذ سنتين و34 ضحية منذ 3 سنوات، يليه سوق العملة الإلكتروني (بيع العملة الافتراضية) وتعارض مع وعي أفراد العينة حيث كان في المرحلة الأخيرة، فهذا من شأنه أن يؤدي إلى زيادة ضحايا العملة الافتراضية نتيجة للجهل من قبل أفراد العينة، ووصل عدد الضحايا 167 ضحية بنسبة 20.39% انقسموا إلى 96 ضحية تعرّضوا للاحتيال سوق العملة الإلكتروني (بيع العملة الافتراضية) منذ أقل من 12 شهر و47 ضحية منذ سنتين، و24 ضحية منذ 3 سنوات، يليه الاحتيال الإلكتروني عن طريق موظفي المصارف وصل عدد الضحايا 159 ضحية بنسبة 19.41% انقسموا إلى 77 ضحية تعرضوا للاحتيال الإلكتروني عن طريق موظفي المصارف منذ أقل من 12 شهر، و43 ضحية منذ سنتين، و39 ضحية منذ 3 سنوات، يليه الاحتيال عن طريق الإعلان عن الوظائف الوهمية حيث وصل عدد الضحايا 155 ضحية بنسبة 18.93% انقسموا إلى 89 ضحية تعرضوا للاحتيال عن طريق الإعلان عن الوظائف الوهمية منذ أقل من 12 شهر و47 ضحية منذ سنتين، و19 ضحية منذ 3 سنوات، يليه الاحتيال الإلكتروني عن طريق اليانصيب حيث وصل عدد الضحايا 154 ضحية بنسبة 18.80% انقسموا إلى 80 ضحية تعرضوا للاحتيال الإلكتروني عن طريق اليانصيب منذ أقل من 12 شهر و41 ضحية منذ سنتين و33 ضحية منذ 3 سنوات، يليه تزوير

بطاقة الائتمان حيث وصل عدد الضحايا 100 ضحية بنسبة 12.21% انقسموا إلى 45 ضحية تعرضوا للاحتيال عن طريق تزوير بطاقة الائتمان منذ أقل من 12 شهر، و29 ضحية منذ سنتين و26 ضحية منذ 3 سنوات.

الجدول (12)

دور أفراد العينة في تعرضهم للاحتيال الإلكتروني:

دور أفراد العينة في تعرضهم للاحتيال الإلكتروني	نعم		لا		لا أعلم	
	التكرار	النسبة المئوية	التكرار	النسبة المئوية	التكرار	النسبة المئوية
عدم الوعي بأساليب الاحتيال الإلكتروني يزيد من جرائم الاحتيال الإلكتروني	1700	92.9	63	3.4	67	3.7
الجهل بالتدابير الأمنية لدى المستهلك (الحيطة والحذر من الوقوع ضحية للاحتيال الإلكتروني)	1651	90.2	65	3.6	114	6.2
إهمال الضحايا في التعامل مع بياناتهم الشخصية	1650	90.2	73	4.0	107	5.8
عدم إبلاغ الضحايا عن تعرضهم للاحتيال الإلكتروني	1622	88.6	73	4.0	135	7.4
الثقه الزائدة لدى المستهلك (الدفع قبل الاستلام)	1592	87.0	112	6.1	126	6.9

يشير الجدول (12) إلى ارتفاع الموافقة من أفراد العينة على أنّ للضحية دور في تعرضه للاحتيال الإلكتروني، فجاء العامل الأول على أن عدم الوعي بأساليب الاحتيال الإلكتروني يزيد من جرائم الاحتيال الإلكتروني بنسبة 92.9%، بينما أفادت الدراسة أن معظم أفراد العينة على معرفة بوجود أنواع الاحتيال لربما يعود إلى معرفتهم بها

بعد تعرضهم للاحتيال وجهلهم في السابق بأنواع الاحتيال، أدى ذلك إلى تعرضهم للاحتيال الإلكتروني واتفقت مع دراسة (شوال، 2008م)، فقد توصّلت الدراسة إلى أنّ الجهل بالمحيط الاجتماعي تزيد من احتمالية وقوع الشخص ضحية للجريمة بمتوسط (3.64)، يليه الجهل بالتدابير الأمنية لدى المستهلك (الحيطة والحذر من الوقوع ضحية للاحتيال الإلكتروني)، وإهمال الضحايا في التعامل مع بياناتهم الشخصية واتفقت النتيجة مع الحكيم (2007م) لإهمال ضحايا السرقات في المحافظة على ممتلكاتهم دور في وقوعهم ضحية لجريمة السرقة، واتفقت مع دراسة شوال (2008م) أن إهمال بعض الضحايا في التعامل مع ممتلكاتهم أدى إلى سرقتها بمتوسط حسابي (3.62)، يليه عدم إبلاغ الضحايا عن تعرضهم للاحتيال الإلكتروني بنسبة 88.6% مع دراسة شوال (2008م) حيث توصّلت الدراسة إلى أنّ عدم تعاون بعض الناس في الإبلاغ عن المجرمين يؤدي إلى زيادة أعداد الضحايا بمتوسط حسابي (3.56)، يليه الثقه الزائدة لدى المستهلك (الدفع قبل الاستلام) بنسبة 87%.

الجدول (13)

الإبلاغ بعد التعرض للاحتيال تم إبلاغ:

بعد تعرضك أو بعد تعرض أحد أقاربك للاحتيال قمت بإبلاغ	التكرار	النسبة المئوية
لم أبلغ	360	28.66
الشرطة	226	17.99
الأسرة	181	14.41
الأسرة، الأصدقاء	174	13.85
الأصدقاء	98	7.80
الأسرة، الشرطة	40	3.18
البنك	38	3.03
الأصدقاء، الشرطة	20	1.59
الاتصالات أو دو	6	0.48
البنك، الشرطة	5	0.40

بعد تعرضك أو بعد تعرض أحد أقاربك للاحتيال قمت بإبلاغ	التكرار	النسبة المئوية
حماية المستهلك	5	0.40
السفارة	1	0.08
كل ما سبق	102	8.12
المجموع	1256	100

يشير الجدول (13) إلى ارتفاع أفراد العينة الذين تعرضوا للاحتيال أو تعرض أحد أقاربهم للاحتيال ولم يبلغوا وذلك بنسبة 28.66%، بعد ذلك جاءت نسبة الذين أبلغوا الشرطة بنسبة 17.99% بعد ذلك الأسرة بنسبة 14.41، ويليه من قاموا بإبلاغ الأسرة والأصدقاء 13.85% ثم جاءت نسبة الذين أبلغوا الأصدقاء فقط بنسبة 7.80% يليه الذين أبلغوا الأسرة والشرطة بنسبة 3.18% ثم الذين أبلغوا البنك فقط بنسبة 3.03%، ثم الذين أبلغوا الأصدقاء والشرطة بنسبة 1.59% ثم الذين أبلغو اتصالات أو دو بنسبة 0.48 ثم اشتركوا الذين أبلغوا البنك والشرطة مع الذين أبلغوا حماية المستهلك بنسبة 0.4%، يليه السفارة 0.08% وأخيرًا كل ما سبق 8.12%.

الجدول (14)

أسباب عدم الإبلاغ تمثّلت في الجدول الآتي:

أسباب عدم الإبلاغ	التكرار	النسبة المئوية
قناعتي بأن القانون لا يحمي ضحايا الاحتيال الإلكتروني	237	37.92
عدم اهتمامي بالمبلغ	151	24.16
الخوف من سخرية الآخرين	115	18.4
العملية لم تنجح	53	8.48
كل ما سبق	23	3.68
الخوف من سخرية الآخرين، قناعتي بأن القانون لا يحمي ضحايا الاحتيال الإلكتروني	17	2.72
لأنهم خارج الدولة	12	1.92
الخوف من سخرية الآخرين، عدم اهتمامي بالمبلغ	11	1.76
الإجراءات القانونية الطويلة	3	0.48

النسبة المئوية	التكرار	أسباب عدم الإبلاغ
0.32	2	الخوف من الجناة
0.16	1	لا يوجد لديّ إثبات
100	625	المجموع

يشير الجدول (14) إلى عدد أعلى من الذين لم يبلغوا لأن بعض أفراد العينة أجابوا على أنهم على حسب عدم إبلاغهم للشرطة فقط، وأشار الجدول إلى أنّ أعلى نسبة كانت بسبب قناعتي بأن القانون لا يحمي ضحايا الاحتيال الإلكتروني بنسبة 37.92، أو كما كان يقال أثناء المقابلات القانون لا يحمي المغفلين، يليه عدم اهتمامي بالمبلغ بنسبة 24.16% ربما بسبب دخل أفراد العينة العالي، يليه الخوف من سخرية الآخرين بنسبة 18.4% ثم الذين تعرضوا للاحتيال لكن لم تنجح عملية النصب وتم تفاديها بنسبة 8.84%، يليه جميع ما سبق بنسبة 3.68، ثم الخوف من سخرية الآخرين وقناعتي بأن القانون لا يحمي ضحايا الاحتيال الإلكتروني بنسبة 2.72، ثم لأنهم خارج الدولة بنسبة 1.92% يليه الخوف من سخرية الآخرين، عدم اهتمامي بالمبلغ بنسبة 1.76% ثم الإجراءات القانونية الطويلة بنسبة 0.48 يليه الخوف من الجناة.

المجموع	لا	نعم	هل قمت بالاطلاع على المواد القانونية التي تتعلق بالاحتيال الإلكتروني في مرسوم مكافحة جرائم تقنيه المعلومات؟
100	73.9	26.1	النسبة المئوية
1830	1352	478	التكرارات

وتمثّلوا بضحايا الابتزاز والاحتيال العاطفي ونسبتهم 0.32%، وأخيرًا لا يوجد لديه إثبات بنسبة 0.16%.

الجدول (15)

القانون وضحايا الاحتيال الإلكتروني

إذا تم الاطلاع سيتم الإجابة من قبل أفراد العينة على هذه التساؤلات	نعم		لا		لا أعلم		المجموع	
	التكرار	النسبة المئوية	التكرار	النسبة المئوية	التكرار	النسبة المئوية	التكرار	النسبة المئوية
عدم تعاون الضحايا في الإبلاغ عن عمليات الاحتيال الإلكتروني أدّى إلى زيادتها	418	87.45	26	5.44	34	7.11	478	100
هل تعتقد أن هناك قواعد وتشريعات تحمي ضحايا الاحتيال الإلكتروني؟	395	82.64	36	7.53	47	9.83	478	100
هل تعتقد أن القانون يحمي ضحايا الاحتيال الإلكتروني؟	386	80.75	55	11.51	37	7.47	478	100
عدم تناسب العقوبة التي توقع على الجناة أدى إلى عدم الإبلاغ عن جرائم الاحتيال الإلكتروني	273	57.11	93	19.45	112	23.43	478	100
بعد تعرضك للاحتيال الإلكتروني هل أوجد القانون طريقة تكفل حقّك؟	255	53.35	69	14.43	154	32.22	478	100

يشير الجدول (15) إلى أنّ معظم أفراد العينة على جهل بالمواد القانونية التي تتعلّق بالاحتيال الإلكتروني في مرسوم مكافحة جرائم تقنية المعلومات حيث يتّضح من الجدول أنّ 26.1% فقط على معرفة بالقانون، وأن هناك قانونًا يحمي ضحايا جرائم تقنية المعلومات، في حين أن 73.9% أجابو أنهم لم يطلعوا على القانون، وبعضهم قد قال أثناء المقابلات إنه لا يعلم بوجود هذا القانون.

تمت الإجابة من قبل الأفراد الذين اطلعوا على المواد القانونية التي تتعلّق بالاحتيال الإلكتروني في مرسوم مكافحة جرائم تقنية المعلومات، فأشار الجدول إلى موافقة أفراد العينة على أن عدم تعاون الضحايا في الإبلاغ عن عمليات الاحتيال الإلكتروني أدى إلى زيادتها بنسبة 87.45%، فهذا دليل على أنّ عدم إبلاغ الضحايا يعطي مجالا للجناة للتمادي في ارتكاب المزيد من الجرائم في حق ضحايا آخرين، يليه: هل تعتقد أن هناك قواعد وتشريعات تحمي ضحايا الاحتيال الإلكتروني؟ وأجابوا بنعم 82.64%، فالمتابع للقانون يلاحظ وجود تشريعات وقوانين كثيرة تحمي ضحايا الاحتيال الإلكتروني ولكن معظم أفراد المجتمع يجهلونها، يليه: هل تعتقد أن القانون يحمي ضحايا الاحتيال الإلكتروني؟ أجابوا بنعم بنسبة 80.75%، بعد ذلك عدم تناسب العقوبة التي توقع على الجناة أدى إلى عدم الإبلاغ عن جرائم الاحتيال الإلكتروني، أجابوا بنعم بنسبة 57.11%، أخيرًا السؤال الذي وجهه للضحايا وأقاربهم بعد تعرضك للاحتيال الإلكتروني هل أوجد القانون طريقة تكفل حقك؟ أجابوا بنعم بنسبة 53.35%.

هل يختلف تعرض أفراد العينة للاحتيال الإلكتروني حسب كل من متغيرات: (النوع الاجتماعي، والعمر، والمستوى التعليمي، والجنسية)؟

الجدول (16)

العلاقة بين المتغيرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال الإلكتروني

المتغيرات	X^2	الدلالة الإحصائية
العمر	9.386^a	.095

الدلالة الإحصائية	X^2	المتغيرات
.089	2.886[a]	الجنس
.129	30.748[a]	الجنسية
.038	13.341[a]	المستوى التعليمي

يشير الجدول إلى عدم وجود علاقة ذات دلالة إحصائية بين التعرض للاحتيال الإلكتروني وبين العمر حيث إنّ (a= 0.095)، كما يشير الجدول إلى عدم وجود علاقة ذات دلالة إحصائية بين التعرض للاحتيال الإلكتروني وبين الجنس (a=0.089)، يشير الجدول أن ليس هناك علاقة ذات دلالة إحصائية بين الجنسية والتعرض للاحتيال الإلكتروني حيث إنه (a=0.129)، حيث إنه لا يوجد علاقة بين العمر، الجنس، الجنسية والتعرض للاحتيال، فعدد الذين تعرضوا للاحتيال من جميع الفئات يعتبر متساويًا مقارنة بعدد العينة، وهذا يعني أن جميع الفئات العمرية والجنسيات والذكور والإناث يتعرّضون لأحد أنواع الاحتيال الإلكتروني. وأشار الجدول إلى وجود علاقة ذات دلالة إحصائية بين المستوى التعليمي والتعرض للاحتيال، حيث إنه (a=0.038).

الجدول (17)

العلاقة بين المتغيرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال الإلكتروني عبر بيع العملة الافتراضية

الدلالة الإحصائية	X^2	المتغيرات
.591	8.389[a]	العمر
.574	1.110[a]	الجنس
.115	27.781[a]	الجنسية
.518	11.127[a]	المستوى التعليمي

يبيّن الجدول العلاقة بين المتغيرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال الإلكتروني عبر بيع العملة الافتراضية، وأشار إلى عدم وجود علاقة ذات دلالة إحصائية بين العمر والتعرض للاحتيال الإلكتروني عبر بيع

العملة الافتراضية، حيث إنه (a=0.591)، وأشار الجدول إلى عدم وجود علاقة ذات دلالة إحصائية بين الجنس والتعرض للاحتيال الإلكتروني عبر بيع العملة الافتراضية حيث إنه (a=0.574)، ويبيّن الجدول أن ليس هناك علاقة ذات دلالة إحصائية بين الجنسية والتعرض للاحتيال الإلكتروني عبر بيع العملة الافتراضية، حيث إنه (a=0.115). كما أشار الجدول إلى عدم وجود علاقة ذات دلالة إحصائية بين المستوى التعليمي والتعرض للاحتيال الإلكتروني عبر بيع العملة الافتراضية حيث إنه (a=0.518).

هذا يعني أن جميع أفراد العينة بمختلف أعمارهم وأجناسهم وجنسياتهم ومستواهم التعليمي يتعرضون للاحتيال الإلكتروني عبر بيع العملة الافتراضية بنفس المستوى.

الجدول (18)

العلاقة بين المتغيرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال الإلكتروني عن طريق موظّفي المصارف

المتغيرات	X^2	الدلالة الإحصائية
العمر	10.506^a	.397
الجنس	$.504^a$	.777
الجنسية	24.870^a	.206
المستوى التعليمي	4.194^a	.938

يبيّن الجدول العلاقة بين المتغيّرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال الإلكتروني عن طريق موظّفي المصارف، وأشار إلى عدم وجود علاقة ذات دلالة إحصائية بين العمر والتعرض للاحتيال الإلكتروني عن طريق موظّفي المصارف، حيث إنه (a=0.397). وأشار الجدول على عدم وجود علاقة ذات دلالة إحصائية بين الجنس والتعرض للاحتيال الإلكتروني عن طريق موظّفي المصارف حيث (a=0.777)، وأشار الجدول على عدم وجود علاقة ذات دلالة إحصائية بين المستوى التعليمي والتعرض للاحتيال الإلكتروني عن طريق

موظّفي المصارف، حيث (a=0.938)، كما يشير الجدول إلى أنه ليس هناك علاقة ذات دلالة إحصائية بين الجنسية والتعرض للاحتيال الإلكتروني عن طريق موظّفي المصارف حيث إنه (a=0.206).

هذا يعني أن جميع الفئات العمرية والذكور والإناث وأفراد العينة بمختلف جنسياتهم ومستوياتهم التعليمية يتعرضون للاحتيال الإلكتروني عن طريق موظّفي المصارف بنفس المستوى.

الجدول (19)

العلاقة بين المتغيرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرّض للاحتيال الإلكتروني عن طريق الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان

المتغيرات	X^2	الدلالة الإحصائية
العمر	11.311^a	.334
الجنس	1.378^a	.502
الجنسية	22.596^a	.309
المستوى التعليمي	12.029^a	.283

يبيّن الجدول العلاقة بين المتغيرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال الإلكتروني عن طريق الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان، وأشار إلى عدم وجود علاقة ذات دلالة إحصائية بين العمر والتعرض للاحتيال الإلكتروني بالاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان حيث (a=0.334)، وأشار الجدول إلى عدم وجود علاقة ذات دلالة إحصائية بين الجنس والتعرض للاحتيال الإلكتروني عن طريق سرقة بيانات بطاقة الائتمان حيث (a=0.502). ويشير الجدول إلى أنه ليس هناك علاقة ذات دلالة إحصائية بين الجنسية، والتعرّض للاحتيال الإلكتروني عن طريق الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان، حيث إنه (a=0.309). وأشار الجدول إلى أنه ليس هناك علاقة ذات دلالة إحصائية بين المستوى التعليمي والتعرض للاحتيال

الإلكتروني من خلال الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان حيث (a=0.283)، وهذا يعني أفراد العينة لا تختلف في تعرضها للاحتيال الإلكتروني بالاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان باختلاف فئاتهم العمرية وجنسياتهم وأعمارهم، وسواء كانوا ذكورًا أم إناثًا فجميعهم يتعرضون للاحتيال الإلكتروني عن طريق سرقة بيانات بطاقة الائتمان بنفس المستوى.

الجدول (20)

العلاقة بين المتغيرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال الإلكتروني عن طريق تزوير بطاقة الائتمان

المتغيرات	X^2	الدلالة الإحصائية
العمر	11.154^a	.346
الجنس	1.190^a	.552
الجنسية	11.497^a	.778
المستوى التعليمي	10.376^a	.408

بيّن الجدول العلاقة بين المتغيرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال الإلكتروني عن طريق تزوير بطاقة الائتمان، وأشار إلى عدم وجود علاقة ذات دلالة إحصائية بين العمر والتعرض للاحتيال الإلكتروني عن طريق تزوير بطاقة الائتمان حيث (a=0.346) ، وأشار الجدول إلى عدم وجود علاقة ذات دلالة إحصائية بين الجنس والتعرض للاحتيال الإلكتروني عن طريق تزوير بطاقة الائتمان حيث (a=0.552)، يشير الجدول أن ليس هناك علاقة ذات دلالة إحصائية بين الجنسية والتعرض للاحتيال الإلكتروني عن طريق تزوير بطاقة الائتمان، حيث إنه (a=0.778). كما بيّن الجدول أنه ليس هناك علاقة ذات دلالة إحصائية بين المستوى التعليمي والتعرض للاحتيال الإلكتروني من خلال تزوير بطاقة الائتمان، حيث (a=0.408) .

هذا يعني أفراد العينة لا تختلف في تعرّضها للاحتيال الإلكتروني عن طريق تزوير بطاقة الائتمان باختلاف الفئات العمرية والجنسيات والجنس والمستوى.

الجدول (21)

العلاقة بين المتغيرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للإحتيال الإلكتروني التجاري، وذلك من خلال التسوق الإلكتروني

المتغيرات	X^2	الدلالة الإحصائية
العمر	16.026[a]	.099
الجنس	5.375[a]	.068
الجنسية	30.846[a]	.324
المستوى التعليمي	7.094[a]	.717

يشير الجدول إلى توزيع أفراد العينة حسب العلاقة بين (العمر والجنس والجنسية والمستوى التعليمي) والتعرض للاحتيال الإلكتروني التجاري وذلك من خلال التسوق الإلكتروني، ويبيّن الجدول عدم وجود علاقة ذات دلالة إحصائية بين العمر والتعرض للاحتيال الإلكتروني التجاري، وذلك من خلال التسوق الإلكتروني حيث كان (a=0.099)، كما أشار الجدول إلى عدم وجود علاقة ذات دلالة إحصائية بين الجنس والتعرض للاحتيال الإلكتروني التجاري، وذلك من خلال التسوّق الإلكتروني حيث (a=0.068)، كما بيّن الجدول أن ليس هناك علاقة ذات دلالة إحصائية بين الجنسية والتعرض للاحتيال الإلكتروني التجاري وذلك من خلال التسوق الإلكتروني، حيث إنه (a=0.324)، كما أشار الجدول أنه ليس هناك علاقة ذات دلالة إحصائية بين المستوى التعليمي والتعرض للاحتيال الإلكتروني التجاري وذلك من خلال التسوق الإلكتروني، حيث كان معامل كاي تربيع (a=0.717).

هذا يعني أنّ أفراد العينة لا تختلف في تعرضها للاحتيال الإلكتروني التجاري وذلك من خلال التسوق الإلكتروني باختلاف الفئات العمرية والجنس والجنسية والمستوى التعليمي.

الجدول (22)

العلاقة بين المتغيرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال الإلكتروني عن طريق الشركات

المتغيرات	X^2	الدلالة الإحصائية
العمر	22.501^a	.013
الجنس	14.405^a	.001
الجنسية	28.189^a	.454
المستوى التعليمي	9.753^a	.462

يشير الجدول إلى توزيع أفراد العينة حسب العلاقة بين (العمر والجنس والجنسية والمستوى التعليمي) والتعرض للاحتيال الإلكتروني عن طريق الشركات، فيبيّن وجود علاقة ذات دلالة إحصائية بين العمر والتعرض للاحتيال الإلكتروني عن طريق الشركات حيث (a=0.013)، وأشار الجدول إلى وجود علاقة ذات دلالة إحصائية بين الجنس والتعرض للاحتيال الإلكتروني عن طريق الشركات (a=0.001). يشير الجدول أن ليس هناك علاقة ذات دلالة إحصائية بين الجنسية والتعرض للاحتيال الإلكتروني عن طريق الشركات، حيث إنه (a=0.454)، وأشار الجدول أنه ليس هناك علاقة ذات دلالة إحصائية بين المستوى التعليمي والتعرض للاحتيال الإلكتروني عن طريق الشركات حيث (a=0.462).

وهذا يعني أن أفراد العينة تختلف في تعرّضها للاحتيال الإلكتروني عن طريق الشركات باختلاف الفئات العمرية والجنس، ولا تختلف في تعرّضها للاحتيال الإلكتروني عن طريق الشركات باختلاف الجنسية والمستوى التعليمي.

الجدول (23)

العلاقة بين المتغيرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للإحتيال الإلكتروني عن طريق المحافظ الاستثمارية الوهمية الإلكترونية

المتغيرات	X^2	الدلالة الإحصائية
العمر	7.855^a	.643
الجنس	1.880^a	.391
الجنسية	21.427^a	.372
المستوى التعليمي	10.405^a	.406

يشير الجدول إلى توزيع أفراد العينة حسب العلاقة بين (العمر والجنس والجنسية والمستوى التعليمي) والتعرض للاحتيال الإلكتروني عن طريق المحافظ الاستثمارية الوهمية الإلكترونية، وأشار الجدول إلى عدم وجود علاقة ذات دلالة إحصائية بين العمر والتعرض للاحتيال الإلكتروني عن طريق المحافظ الاستثمارية الوهمية الإلكترونية حيث (a=0.643) ، وأشار الجدول إلى عدم وجود علاقة ذات دلالة إحصائية بين الجنس والتعرض للاحتيال الإلكتروني عن طريق المحافظ الاستثمارية الوهمية الإلكترونية (a=0.391) ، ويشير الجدول أن ليس هناك علاقة ذات دلالة إحصائية بين الجنسية والتعرض للاحتيال عن طريق المحافظ الاستثمارية الوهمية الإلكترونية، حيث إنه (a=0.372). ويبيّن الجدول أنه ليس هناك علاقة ذات دلالة إحصائية بين المستوى التعليمي والتعرض للاحتيال الإلكتروني عن طريق المحافظ الاستثمارية الوهمية الإلكترونية (a=0.406).

وهذا يعني أنّ أفراد العينة لا تختلف في تعرضها للاحتيال الإلكتروني عن طريق المحافظ الاستثمارية الوهمية الإلكترونية باختلاف الفئات العمرية والجنس والجنسية والمستوى التعليمي.

الجدول (24)

العلاقة بين المتغيرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للإحتيال الإلكتروني عن طريق الاعلان عن الوظائف الوهميه

المتغيرات	X^2	الدلالة الإحصائية
العمر	8.159^a	.613
الجنس	3.627^a	.163
الجنسية	25.712^a	.589
المستوى التعليمي	6.917^a	.863

يشير الجدول إلى توزيع أفراد العينة حسب العلاقة بين (العمر والجنس والجنسية والمستوى التعليمي) والتعرض للاحتيال الإلكتروني عن طريق الإعلان عن الوظائف الوهمية، ويبيّن الجدول أنه ليس هناك علاقة ذات دلالة إحصائية بين العمر والتعرض للاحتيال الإلكتروني عن طريق الإعلان عن الوظائف الوهمية حيث (a=0.613)، وأشار الجدول إلى عدم وجود علاقة ذات دلالة إحصائية بين الجنس والتعرض للاحتيال الإلكتروني عن طريق الإعلان عن الوظائف الوهمية (a=0.163)، كما يشير الجدول أن ليس هناك علاقة ذات دلالة إحصائية بين الجنسية والتعرض للاحتيال عن طريق الإعلان عن الوظائف الوهمية، حيث إنه (a=0.589). وأشار الجدول أنه ليس هناك علاقة ذات دلالة إحصائية بين المستوى التعليمي والتعرض للاحتيال الإلكتروني عن طريق الإعلان عن الوظائف الوهمية حيث كان (a=0.863).

وهذا يعني أنّ أفراد العينة لا تختلف في تعرضها للاحتيال الإلكتروني عن طريق الإعلان عن الوظائف الوهمية باختلاف الفئات العمرية والجنس والجنسية والمستوى التعليمي.

الجدول (25)

العلاقة بين المتغيّرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال الإلكتروني عن طريق انتحال صفة كبار الشخصيات

المتغيرات	X^2	الدلالة الإحصائية
العمر	12.113[a]	.278
الجنس	3.911[a]	.142
الجنسية	27.962[a]	.262
المستوى التعليمي	27.245[a]	.007

يشير الجدول إلى توزيع أفراد العينة حسب العلاقة بين (العمر، الجنس،المستوى التعليمي، الجنسية) والتعرض للاحتيال الإلكتروني عن طريق انتحال صفة كبار الشخصيات، ويبيّن الجدول عدم وجود علاقة ذات دلالة إحصائية بين العمر والتعرض للاحتيال الإلكتروني عن طريق انتحال صفة كبار الشخصيات حيث (a=0.278). وأشار الجدول إلى عدم وجود علاقة ذات دلالة إحصائية بين الجنس والتعرض للاحتيال الإلكتروني عن طريق انتحال صفة كبار الشخصيات (a=0.142). ويشير الجدول أن ليس هناك علاقة ذات دلالة إحصائية بين الجنسية والتعرض للاحتيال عن طريق انتحال صفة كبار الشخصيات حيث إنه (a=0.262). وأشار الجدول أن هناك علاقة ذات دلالة إحصائية بين المستوى التعليمي والتعرض للاحتيال الإلكتروني عن طريق انتحال صفة كبار الشخصيات حيث (a=0.007).

وهذا يعني أن أفراد العينة لا تختلف في تعرضها للاحتيال الإلكتروني عن طريق انتحال صفة كبار الشخصيات باختلاف الفئات العمرية والجنس والجنسية تختلف في تعرضها للاحتيال الإلكتروني عن طريق انتحال صفة كبار الشخصيات باختلاف المستوى التعليمي.

الجدول (26)

العلاقة بين المتغيرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال الإلكتروني عن طريق التسوّل الإلكتروني

المتغيرات	X^2	الدلالة الإحصائية
العمر	29.346^a	.001
الجنس	7.869^a	.020
الجنسية	41.980^a	.044
المستوى التعليمي	10.007^a	.615

يشير الجدول إلى توزيع أفراد العينة حسب العلاقة بين (العمر، الجنس،المستوى التعليمي، الجنسية) والتعرض للاحتيال الإلكتروني عن طريق التسول الإلكتروني، ويبيّن وجود علاقة ذات دلالة إحصائية بين العمر والتعرض للاحتيال الإلكتروني عن طريق التسول الإلكتروني حيث (a=0.001). وأشار الجدول إلى وجود علاقة ذات دلالة إحصائية بين الجنس والتعرض للاحتيال الإلكتروني عن طريق التسول الإلكتروني (a=0.020)، ويشير الجدول أن هناك علاقة ذات دلالة إحصائية بين الجنسية والتعرض للاحتيال عن طريق التسول الإلكتروني حيث إنه (a=0.044)، وأشار الجدول أن ليس هناك علاقة ذات دلالة إحصائية بين المستوى التعليمي والتعرض للاحتيال الإلكتروني عن طريق التسول الإلكتروني حيث (a=0.615).

وهذا يعني أن أفراد العينة تختلف في تعرضها للاحتيال الإلكتروني عن طريق التسول الإلكتروني باختلاف الفئات العمرية والجنس والجنسية ولا تختلف في تعرضها للاحتيال الإلكتروني عن طريق التسول الإلكتروني باختلاف المستوى التعليمي.

الجدول (27)

العلاقة بين المتغيرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال الإلكتروني العاطفي

المتغيرات	X^2	الدلالة الإحصائية
العمر	6.933[a]	.732
الجنس	.384[a]	.825
الجنسية	18.647[a]	.771
المستوى التعليمي	9.900[a]	.625

يشير الجدول إلى توزيع أفراد العيّنة حسب العلاقة بين (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال الإلكتروني العاطفي، فيبين أنه ليس هناك علاقة ذات دلالة إحصائية بين العمر والتعرض للاحتيال الإلكتروني العاطفي حيث (a=0.732). وأشار الجدول إلى عدم وجود علاقة ذات دلالة إحصائية بين الجنس والتعرض للاحتيال الإلكتروني العاطفي (a=0.825)، ويشير الجدول أنه ليس هناك علاقة ذات دلالة إحصائية بين الجنسية والتعرض للاحتيال الإلكتروني العاطفي حيث إنه (a=0.771) . وأشار الجدول أن ليس هناك علاقة ذات دلالة إحصائية بين المستوى التعليمي والتعرض للاحتيال الإلكتروني عن طريق الاحتيال العاطفي حيث كان (a=0.625).

وهذا يعني أن أفراد العينة لا تختلف في تعرضها للاحتيال الإلكتروني عن طريق الاحتيال العاطفي باختلاف الفئات العمرية والجنس والجنسية والمستوى التعليمي.

الجدول (28)

العلاقة بين المتغيرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال والنصب عبر الهاتف

المتغيرات	X^2	الدلالة الإحصائية
العمر	13.558^a	.194
الجنس	2.480^a	.289
الجنسية	43.919^a	.078
المستوى التعليمي	9.048^a	.699

يشير الجدول إلى توزيع أفراد العينة حسب العلاقة بين (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال والنصب عبر الهاتف، فيبيّن أنه ليس هناك علاقة ذات دلالة إحصائية بين العمر والتعرض للاحتيال والنصب عبر الهاتف، حيث إنه (a=0.194). وأشار الجدول إلى عدم وجود علاقة ذات دلالة إحصائية بين الجنس والتعرض للاحتيال والنصب عبر الهاتف (a=0.289). كما يشير الجدول أن ليس هناك علاقة ذات دلالة إحصائية بين الجنسية والتعرض للاحتيال والنصب عبر الهاتف حيث إنه (a=0.078). وأشار الجدول أن ليس هناك علاقة ذات دلالة إحصائية بين المستوى التعليمي والتعرض للاحتيال والنصب عبر الهاتف حيث كان (a=0.699)؛ أي: أن التعرض للاحتيال والنصب عبر الهاتف لا يختلف باختلاف الفئات العمرية والجنس والجنسية والمستوى التعليمي.

الجدول (29)

العلاقة بين المتغيرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي

المتغيرات	X^2	الدلالة الإحصائية
العمر	9.143^a	.519
الجنس	8.848^a	.012
الجنسية	36.781^a	.124
المستوى التعليمي	7.695^a	.808

يشير الجدول إلى توزيع أفراد العينة حسب العلاقة بين (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال عبر وسائل التواصل الاجتماعي، فيبيّن أنه ليس هناك علاقة ذات دلالة إحصائية بين العمر والتعرض للاحتيال عبر وسائل التواصل الاجتماعي حيث كان (a=0.519)، وأشار الجدول إلى وجود علاقة ذات دلالة إحصائية بين الجنس والتعرض للاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي (a=0.012). كما يشير الجدول أن ليس هناك علاقة ذات دلالة إحصائية بين الجنسية والتعرض للاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي حيث إنه (a=0.124) . وأشار الجدول أن ليس هناك علاقة ذات دلالة إحصائية بين المستوى التعليمي والتعرض للاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي حيث (a=0.808)؛ أي: أن التعرض للاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي لا يختلف باختلاف الفئات العمرية والجنسية والمستوى التعليمي والتعرض للاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي يختلف باختلاف الجنس.

الجدول (30)

العلاقة بين المتغيرات الأولية (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال الإلكتروني عبر اليانصيب

المتغيرات	X^2	الدلالة الإحصائية
العمر	6.432[a]	.778
الجنس	.182[a]	.913
الجنسية	19.491[a]	.725
المستوى التعليمي	16.583[a]	.166

يشير الجدول إلى توزيع أفراد العينة حسب العلاقة بين (العمر، الجنس، المستوى التعليمي، الجنسية) والتعرض للاحتيال عن طريق اليانصيب، فيبين أنه ليس هناك علاقة ذات دلالة إحصائية بين العمر والتعرض للاحتيال عن طريق اليانصيب حيث (a=0.778)، وأشار الجدول إلى عدم وجود علاقة ذات دلالة إحصائية بين الجنس

والتعرض للاحتيال الإلكتروني عن طريق اليانصيب (a=0.913)، كما يشير الجدول أن ليس هناك علاقة ذات دلالة إحصائية بين الجنسية والتعرض للاحتيال الإلكتروني عبر اليانصيب حيث إنه (a=0.725)، وأشار الجدول أن ليس هناك علاقة ذات دلالة إحصائية بين المستوى التعليمي والتعرض للاحتيال الإلكتروني عبر اليانصيب حيث كان (a=0.166)؛ أي: أنّ التعرّض للاحتيال الإلكتروني عن طريق اليانصيب لا يختلف باختلاف الفئات العمرية والجنسية والمستوى التعليمي والجنس.

الفصل الثالث
مناقشة النتائج

مناقشة النتائج

الخصائص الديموجرافية والاجتماعية والاقتصادية لأفراد العينة:

تمثّلت خصائص أفراد العينة في الآتي: حيث مثّلت الفئة العمرية من 18 إلى أقل من 30 سنة أعلى فئة عمرية من أفراد العينة بنسبة 50%، فمعظم أفراد العينة يعتبرون من فئة الشباب، أمّا بالنسبة لجنس المبحوثين فتمثّلت نسبة الإناث بنسبة 58.4%، أمّا الذكور فقد شكّلوا نسبة 41.6%. وبالنظر للحالة الاجتماعية بالنسبة للمبحوثين فتمثّلت بارتفاع أفراد العينة العازبون بنسبة 51.4%، وأقل فئة الأرامل بنسبة 0.6%. أمّا توزيع أفراد العينة بحسب محل الإقامة فجاء المقيمون في إمارة الشارقة بنسبة 27.2%، وفي إمارة دبي بنسبة 23.8 %، وفي إمارة أبوظبي بنسبة 22.2% ثم إمارة عجمان بنسبة 10.8%، إمارة رأس الخيمة بنسبة 5.7%، إمارة أم القيوين، وكانت نسبتهم 5.5% وجاءت أقل نسبة الفجيرة بنسبة 4.8%. ويشير الجدول إلى ارتفاع أفراد العينة في مستوى البكالوريوس بنسبة 56.1%، و أخيرًا أمّيّ 0.3%. وذلك بسبب تركيز توزيع الاستبيان في الجامعات والدوائر الحكومية، لهذا ظهرت نسبة المستويات العلمية عالية. تمثّلت مهنة أفراد العينة بأعلى نسبة في مهن القطاع الحكومي بنسبة 48.3%، وأقل نسبة للأعمال الحرة بنسبة 2.1%. وجاءت نسب دخل أفراد العينة متقاربة فارتفاع أفراد العينة الذين دخلهم من 10000 - أقل من 20000بنسبة 27.6%، ويليه أفراد العينة الذين دخلهم أقل من 10000 بنسبة 26.6%، ويليه أفراد العينة الذين دخلهم من20000 - أقل من 30000 بنسبة 23.7%، وأخيرًا 30000 فأكثر بنسبة 22.1%. ارتفاع أفراد العينة الذين مصدر دخلهم من خلال العمل بنسبة 79%، وأقل نسبة لعمل الابنة 0.1%. وتمثّلت أعلى

نسبة في أفراد العينة من حيث المسكن في الذين يسكنون في فيلا بنسبة 54.8%، وأقل نسبة سكن جامعي 0.3%. أمّا جنسية أفراد العيّنة فتمثّلت أعلى في الجنسية الإماراتية بنسبة 69.9% وأقل نسبة من الجنسيات الآتية موريتانيا، كندا، فرنسا، بريطانيا، حيث شكلوا 0.1%.

هل أفراد العينة على دراية ووعي بأنواع الاحتيال الإلكتروني، وما أنماط الاحتيال الإلكتروني التي سبق وتعرض لها أفراد العينة، وما الأنماط التي سبق أن تعرض لها أقرباء وأصدقاء أفراد العينة؟

كشفت الدراسة ارتفاع وعي أفراد العينة وإدراكهم بأنماط الاحتيال الإلكتروني وصوره الشائعة بالمجتمع الإماراتي، وهذا له علاقة في التعرض للاحتيال الإلكتروني فمعظم أفراد العينة قد تعرّضوا أو تعرض أحد أقاربهم أو أصدقائهم للاحتيال الإلكتروني فنتيجة لجهلهم في السابق تعرضوا للاحتيال الإلكتروني وجاءت المعرفة بالاحتيال بعد التعرض له أو بعد تعرض أحد الأقارب، فنتيجة لانتشار جرائم الاحتيال الإلكتروني وزيادة التوعية بها من خلال الجهات الأمنية زاد الوعي لدى أفراد المجتمع، فقد أظهرت الدراسة أن أعلى نسبة في ضحايا الاحتيال الإلكتروني هي الاحتيال والنصب عبر الهاتف، حيث وصلت نسبة الضحايا الذين تعرضوا للاحتيال والنصب عبر الهاتف 46.63% من مجموع الضحايا، أمّا أقارب وأصدقاء أفراد العينة من ضحايا الاحتيال والنصب عبر الهاتف فقد بلغت نسبتهم 44.93%، وتوافق مع إدراك أفراد العينة، حيث كانت أعلى نسبة الاحتيال والنصب عبر الهاتف، فقد شكلت نسبة الذين أجابوا بأنه موجود 93.8%، وإنّ سبب ارتفاع المعرفة بهذا النوع من الاحتيال يعود لانتشاره فلا يوجد شخص لم تصله رسائل هاتفية تفيد بأنه ربح مبالغ مالية أو جوائز قيمة، وهناك الكثير من الناس الذين يصدقونهم ويقومون بتحويل مبالغ لهم. وأكّد ذلك عدد من الحالات (الحالة الاثنين والثلاثين)، (الحالة الثالثة والثلاثين)، (الحالة الرابعة والثلاثين)، (الحالة الخامسة والثلاثين) حيث تعرضوا لعملية نصب من أشخاص أخبروهم بأنهم قد ربحوا مبالغ مالية ضخمة، وليتم إرسالها يجب أن يقوموا بتحويل

مبالغ مالية مقابل تسليمهم الجائزة نتيجة لجهلهم في السابق بهذا النوع من الاحتيال الإلكتروني. ويفسر هذا النوع من الاحتيال الضحية المولع بالاكتساب فيتم خداعه بأنه ربح مبلغًا ماليًّا، وليتم تحويلها يجب أن يرسل لهم مبلغا نقديا، فلولعه باكتساب المال يقوم بتحويل الأموال لهم ظنًّا منه أنه فعلاً ربح مبالغ مالية كبيرة.

توافق بشكلٍ تقريبي إدراك أفراد العينة للاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي حيث جاء في المرتبة الثانية الوعي بالاحتيال مع التعرض للاحتيال بشكلٍ شخصي، حيث جاء في المرتبة الثالثة، وتعرض الأقارب للاحتيال في المرتبة الثانية، وشكّلت نسبة الذين أجابوا بأنه موجود 88.7%. ويعود ارتفاع الوعي إلى زيادة اختراق وسائل التواصل الاجتماعي وطلب المال من أصدقاء الضحية، ووصلت نسبة الضحايا الذين تعرضوا للاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي إلى 34.22%، أمّا بالنسبة لأقارب أفراد العينة الذين تعرضوا للاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي فوصلت نسبة الضحايا إلى 35.04%، وأكّد ذلك عدد من الحالات تمثلت في (الحالة السادسة والثلاثين)، (الحالة السابعة والثلاثين)،(الحالة الثامنة والثلاثين)، (الحالة التاسعة والثلاثين) حيث إنهم جميعهم قد تعرضوا للاحتيال والنصب عبر اختراق إحدى وسائل التواصل الاجتماعي نتيجة لإرسال رابط لهم، ونتيجة عدم وعيهم قاموا بالنقر عليه أو بطلب بيانات خاصة، وتم إعطائها للمحتال فقام باختراق أجهزتهم وانتحل شخصيتهم وبدأ يطالب بأموال من أصدقائهم، فنتيجة لجهلهم في السابق أدى إلى وقوعهم ضحية وتم الاحتيال عليهم باختراق حسابهم وأخذ أموال من أقاربهم وأصدقائهم، ويتّضح ذلك أكثر من خلال الضحية المسهل، فقد قام الضحية هنا بالتواصل مع الجاني وأعطاه البيانات التي تسهّل اختراق جهازه، ممّا أدّى إلى وقوعه ضحية للاحتيال.

وجاء الاحتيال الإلكتروني العاطفي في الوعي بأنواع الاحتيال الإلكتروني في المرحلة الثالثة، حيث شكّلت نسبة الذين أجابوا بأنه موجود 86%، أما بالنسبة للضحايا الذين تعرّضوا بشكلٍ شخصي فلم يتوافقوا مع وعي أفراد العينة بشكلٍ كبير حيث جاء

الاحتيال الإلكتروني العاطفي في المرحلة السابعة من أنواع الاحتيال التي تعرض لها أفراد العينة ووصلت نسبة الضحايا إلى 21.45%، أمّا بالنسبة للأنواع التي تعرض لها أقارب وأصدقاء أفراد العينة فجاء الاحتيال الإلكتروني العاطفي في المرتبة الخامسة حيث وصلت نسبة الضحايا إلى 27.11% من مجموع الضحايا الذي يبلغ 819، فانتشرت العلاقات العاطفية من خلال الإنترنت، ويتم ذلك عندما يبني المحتال علاقة قوية على الإنترنت مع شخص ما، ويتم إقناع الضحية بإرسال صوره أو أي بيانات آخرى للمحتال، ويقوم المحتال بطلب أموال لعدم نشر المحتوى، واختلاف وعي الأفراد بأنواع الاحتيال الإلكتروني والتعرض له جاء بنسبة بسيطة لعدة أسباب: أولا: بسبب انتشار هذا النوع من الاحتيال الإلكتروني فأصبح أفراد المجتمع على وعي به فإذا لم يتعرض الشخص له فقد يتعرض أحد أقاربه وأصدقائه، واتضح ذلك أثناء المقابلات فإذا لم يتعرض الشخص له فقد تعرض له أحد أقاربه، فيفصح عما حدث.

وأيضًا نتيجة لانتشار هذا النوع وزيادة التوعية به من خلال وسائل الإعلام زاد الوعي به، وأيضًا الاحتيال العاطفي الذي يعتبر في المجتمع الإماراتي من المواضيع الحساسة التي لا يفشي بها أيّ شخص، فربما كان العدد أكبر ولكن بسبب الخوف من إفشاء هذا السر حتى في البحوث العلمية بسبب العادات والتقاليد التي تحرم العلاقة بين الذكر والأنثى، وهذا يعدّ وصمة اجتماعية تلاحقهم طيلة حياتهم إذا عرف بها المجتمع، فلهذا لا يتم إفشاء الأمر والتكتم عليه وعدم قوله لأيّ شخص، وأكّد ذلك الحالات الآتية: (الحالة العشرون)، (الحالة الحادية والعشرون)، (الحالة الثالثة والعشرون)، (الحالة الرابعة والعشرون)، (الحالة الخامسة والعشرون)، حيث إنهم جميعًا تعرضوا للاحتيال الإلكتروني العاطفي وذلك من خلال إنشاء علاقة عاطفية على الإنترنت، وإنّ الضحية (الحالة العشرون) حيث إنه قام بعلاقة جنسية مع إحدى الفتيات على سكايب وسجلت الفتاة محادثة الفيديو وهدّدت بنشرها للأصحاب والأهل عبر الانستقرام، كما نشرتها على يوتيوب، فتعرض الشاب لهذا النوع من الاحتيال بخداعه من قبل الفتاة للقيام بعلاقة جنسية مصورة، وتم استغلالها ضده، وأكّد ذلك أيضًا حالة الفتاتين في الحالة

الحادية والعشرين والحالة الخامسة والعشرية، حيث إنه كانت حالتهم مقاربة فتعرفوا على شاب من خلال وسائل التواصل الاجتماعي في حين مرورهم بظروف نفسية سيئة فقام الشباب باستغلال وضعهم النفسي وإيهامهم بأنهم يحبونهم، الأمر الذي جعلهم يقومون بالتصوير لهم، بعد ذلك قام الشباب بابتزاهم، وأيضًا أكّدت ذلك الحالة الثانية والعشرون والثالثة والعشرون والرابعة والعشرون من تعرضهم للابتزاز نتيجة لإقامة علاقة مع شاب بالإنترنت وإرسال صورهم له، بعد ذلك يقوم بطلب أموال مقابل عدم نشر صورهم، فقام الضحايا بإقامة هذه العلاقات نتيجة عدم الوعي بوجود هؤلاء الأشخاص الذين يقومون باستغلال مشاعر الناس وظروفهم في سبيل تحقيق أهدافهم، الأمر الذي أدّى بهم للوقوع ضحايا للاحتيال الإلكتروني، ويفسّر هذا النوع من الاحتيال الضحية المسهل، فالضحية هنا قد تواصل مع الجاني، وهو من قام بإرسال صوره وبياناته للجاني الذي قام بدوره باستغلالها ضده.

توافق بشكلٍ تقريبي الوعي في التسول الإلكتروني مع التعرض لاحتيال الإلكتروني، حيث جاء الوعي في المرتبة الرابعة وشكّلت نسبة الذين أجابوا بأنه موجود 85.2% وتعرض أفراد العينة للتسول الإلكتروني في المرتبة الخامسة حيث وصلت نسبة الضحايا 29.96%، بينما احتل تعرض أقارب وأصدقاء أفراد العينة الرتبة السابعة حيث وصلت نسبة الضحايا إلى 23.81%، ويتم ذلك بادعاء أشخاص للفقر عن طريق وسائل التواصل الاجتماعي وهم ليسو بفقراء، فانتشر هذا النوع في المجتمعات الخليجية من خلال عصابات من مجتمعات عربية، وغالبًا ما يتم استغلال النساء لجذب عاطفة الناس حيث تظهر النساء فقرهن وفقر أبنائهن، وأنهن لا يجدن قوت يومهن. الأمر الذي من شأنه أن يجعل الناس يتعاطفون معهن ويقومون بإرسال مبالغ لهن، وأكد ذلك (الحالة الثلاثون)، (الحالة الحادية والثلاثين) حيث إنهم تعرضوا للاحتيال عبر التسول الإلكتروني من خلال ادعاء نساء من جنسيات عربية أنهن فقيرات ولا يجدن قوت يومهن، ونتيجة لأنّ الضحايا لا يعرفون بوجود عصابات النصب وقعوا ضحايا للاحتيال الإلكتروني، ويفسر هذا النوع من الاحتيال الضحية

المسهل، فالضحية هنا قد تواصل مع الجاني وقام بإرساله للأموال من دون التأكد من صدقه.

توافق وعي وإدراك أفراد العينة مع التعرض للاحتيال الإلكتروني التجاري وذلك من خلال التسوق الإلكتروني حيث جاء وعي أفراد العينة في هذا النوع في المرتبة الخامسة من أنواع الاحتيال الإلكتروني التي يعرف أفراد المجتمع بوجودها، فشكّلت نسبة الذين أجابوا بأنه موجود 83.4%، في حين تعرض أفراد العينة للاحتيال الإلكتروني وذلك من خلال التسوق الإلكتروني في المرتبة الثانية حيث وصلت نسبة الضحايا إلى 37.59%، أمّا الضحايا من أقارب وأصدقاء أفراد العينة من خلال التسوق الإلكتروني في المرتبة الثالثة حيث بلغت نسبة الضحايا 32.47%، ويتم عند عدم وصول البضاعة بعد الدفع أو وصول بضاعة أخرى بمواصفات آخرى، وأكّد هذا الحالات الآتية (الحالة الثامنة)، (الحالة التاسعة)، (الحالة العاشرو)، (الحالة الحادية عشر)، (الحالة الثانية عشر)، (الحالة الثالثة عشر)، (الحالة الرابعة عشر)، (الحالة الخامسة عشر) فجميعهم تعرضوا للاحتيال الإلكتروني من خلال التسوق الإلكتروني حيث تعرض بعضهم للاحتيال بسبب الدفع قبل الاستلام وعدم وصول البضاعة، وأحد أسباب زيادة الاحتيال الإلكتروني هو الرغبة في سرعة وصول البضاعة وعدم الرغبة في الذهاب للسوق والتسوق حتى عندما نتحدث عن الأمور الباهضة الثمن كما ذكرت الحالتين (الحالة العاشرة) و(الحالة الحادية عشر) حيث قاموا بشراء سيارات من خلال مواقع وتم الدفع قبل الاستلام ولم تصل السيارات، وذكرت الحالة التاسعة أنه عن طريق موقع أنستجرام تم شراء آثاث بيت وتم تحويل المبلغ وبعد ذلك لم يتم استلام الآثاث. وأكدت ذلك أيضًا الحالة الرابعة عشر حيث إنها قامت بشراء غرض عبر الانستا وقامت بالدفع ولم يصل، وأيضًا تعرض صنف آخر من الضحايا للاحتيال وذلك بوصول البضاعة ولكنها مخالفة للمواصفات كالحالة الثامنة، حيث إنه قام بشراء خاتم على أنه ألماس من الأنستغرام وبعدها اكتشفت بأن الخاتم ليس ألماسًا. الحالة الثالثة عشر اشترى هاتفًا عن طريق الإنترنت واتضح بعد ذلك أنه (صيني)، والحالة

الثانية عشر طلب من موقع إلكتروني بطاريات بكميات كبيرة ومدعين بأنها أصلية وعندما وصلت اكتشف أنها غير أصلية، الحالة الخامسة عشر عن طريق التسوق الإلكتروني (البضاعة لم تكن كما في العرض وأيضًا السعر مرتفع جدًّا) فتعرض هنا الضحايا للاحتيال الإلكتروني نظرًا لعصر السرعة والرغبة في إنهاء كافة المعاملات عبر الإنترنت، الأمر الذي من شأنه أدى إلى وقوعهم ضحايا للاحتيال، ويفسّر هذا من خلال الضحية المتهور: فمن خلال وضعه لبيانات بطاقته الائتمانية في أي موقع ودفع أموال قبل استلام البضاعة، ولا سيما إذا كانت بضائع باهضة الثمن كما ظهر في بعض الحالات، فهذا يعتبر سلوكًا طائشًا، فكيف يقوم بالدفع قبل أن يستلم البضاعة ويفحصها جيدًا، وبخاصة إذا كانت سيارة أو أثاثًا أو خاتم ألماس، كما ظهر في بعض الحالات.

في المرتبة السادسة جاء الوعي نوع الاحتيال الإلكتروني عن طريق الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان، فشكلت نسبة الذين أجابوا بأنه موجود 82.0% وتوافق مع تعرض أفراد العينة للاحتيال عن طريق الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان، حيث جاء في المرتبة السادسة وبلغت نسبة الضحايا 21.63%، أما الضحايا من أقارب وأصدقاء أفراد العينة الذين تعرضوا للاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان في الرتبه الرابعة، ووصلت نسبة الضحايا إلى 28.82%، ويتم من خلال وضع بيانات بطاقة الائتمان في أجهزة الهواتف الذكية أو في المواقع غير الموثوقة، كما في الحالة الخامسة حيث إنه أثناء تسوقه عن طريق الإنترنت تم سحب مبلغ أقصى من البطاقة، ويفسر بالضحية المتهورة حيث من خلال وضعه لبيانات بطاقته الائتمانية في موقع إلكتروني ودفع أموال قبل استلام البضاعة، وهذا يعتبر سلوكا طائشًا أو يتم إعطاؤها لأشخاص كما في الحالة الرابعة حيث إنه تم الاتصال بها هاتفيًّا والادعاء أنها ربحت مبلغ 100 ألف درهم في أحد السحوبات، وطلبوا رقم الحساب للتحويل وأرادوا بيانات أخرى فأعطتهم فتم سحب رصيدها من البنك الذي بلغ المبلغ 50000 درهم، وتم سحبه بالكامل.

وتفسر هذه الحالة في الضحية المولعة بالاكتساب فأعطتهم الرقم السري ظنًّا منها أنهم سيقومون بتحويل مبلغ مالي لها.

في المرتبة السابعة من وعي وإدراك أفراد العينة جاء انتحال صفة كبار الشخصيات، فشكلت نسبة الذين أجابوا بأنه موجود 80.0%، أمّا الذين تعرضوا لانتحال صفة كبار الشخصيات من أفراد العينة في الرتبة الخامسة حيث وصلت نسبة الضحايا إلى 28%، أمّا تعرض أصدقاء وأقارب أفراد العينة لانتحال صفة كبار الشخصيات المرتبة السادسة، حيث وصلت نسبة الضحايا إلى 24.42%، وذلك من خلال ما انتشر بالفترة الماضية عن طريق وسائل التواصل الاجتماعي بانتحال بعض الشخصيات لصفة شيوخ وطلب تحويل أموال لهم، وهذا ما أكدته الحالة التاسعة والعشرين حيث أكد أنه تعرض للنصب عن طريق شخصية انتحلت شخصية أحد بنات الحكام، وتقول إنها مسافرة وحسابها البنكي محظور وتساعد عائلة فتطلب منه أن يقوم بالتحويل بدلاً منها وعندما تعود ستقوم بإعطائه أضعاف المبلغ. وقام بالتحويل لها وهذا يفسر بالضحية المسهل، إذ إنه تواصل مع الضحية بشكلٍ شخصي وقام بالتحويل دون التأكد ودخل لبيئة لا يعرفها وغير متأكد منها.

في المرتبة الثامنة جاء الاحتيال عن طريق الإعلان عن الوظائف الوهمية، فشكّلت نسبة الذين أجابوا بأنه موجود 76.1%، أمّا الذين تعرضوا للاحتيال عن طريق الإعلان عن الوظائف الوهمية فكان في المرتبة 12 حيث وصلت نسبة الضحايا إلى 17.2%، أما بالنسبة للضحايا من أقارب وأصدقاء أفراد العينة الذين تعرضوا للاحتيال عن طريق الإعلان عن الوظائف الوهمية في المرتبة 12 حيث بلغت نسبة الضحايا إلى 18.93%. فبالنظر إلى النتائج يلاحظ ارتفاع الوعي ولكن ذلك يتناسب مع عدد الضحايا، حيث إنه نتيجة تعرضهم وتعرض غيرهم لهذا النوع من الاحتيال الإلكتروني زاد الوعي بانتشار نوع الجريمة نتيجة لتعرض الأهل والأصدقاء يزيد الوعي بها، كما أكدته الحالة الثامنة والعشرين حيث إنه تم الإعلان عن وظيفة طلب مترجم فقامت بالعمل معهم والقيام بالترجمة لشهر كامل وبعد ذلك لم يتم إعطاؤها المبلغ المتفق عليه،

ويتمثل في الضحية المولع بالاكتساب فمن خلال رغبته في العمل وتحسين وضعه يقوم بالعمل دون التأكد من صدق المعلن ودون عقود ووثائق تثبت حقه.

المرتبة التاسعة جاء الوعي بنوع الاحتيال الإلكتروني عن طريق المحافظ الاستثمارية الوهمية الإلكترونية، فشكلت نسبة الذين أجابوا بأنه موجود 66.8%، وتوافق بشكلٍ تقريبي مع تعرض أفراد العينة للاحتيال عن طريق الاحتيال عن طريق المحافظ الاستثمارية الوهمية الإلكترونية، حيث جاء في المرتبة العاشرة وبلغ عدد الضحايا 17.91%، أمّا الضحايا من أقارب وأصدقاء أفراد العينة الذين تعرضوا للاحتيال عن طريق المحافظ الاستثمارية الوهمية الإلكترونية في المرتبة الثامنة وبلغت نسبة الضحايا 21.61%، ويتم من خلال خداع المحتال للضحية بأنه سيحصل على أرباح كبيرة لمجرد دخوله، وبعد أن يثق به ويدخل ويدخل أعدادا كبيرة من الناس يعلن إفلاس الشركة، وأكد ذلك (الحالة السادسة والعشرين) الذي تعرض للاحتيال عبر موقع www.lesoie.com ويقول إن هذا الموقع يقوم بالنصب على المستثمرين الجدد الذين ليس لديهم خبرة. أول موقع يعطي وكالة ويسأل المستثمر كم الراتب وهل لديك خبرة في المشروع من أقاربك حتى يتمكنون من استغلال المستثمر والاحتيال على أمواله بطريقة قانونية ويتم خداعه بالأرباح الكبيرة، (الحالة السابعة والعشرين) تم خداعه بأنه سيحصل على أرباح كبيرة مع بعض الأفارقة ونصبوا عليه في مليون درهم ثم اختفوا وهربوا من البلاد فورًا بعد إيداع المبلغ في حسابهم خارج الدولة. يفسر هذا في شخصية الضحية المولع بالاكتساب حيث يتم خداع الضحية بأنه سيكسب أرباح كبيرة، وأنه سيتم مضاعفة أمواله.

في المرتبة العاشرة جاء الوعي بنوع الاحتيال الإلكتروني عن طريق اليانصيب فشكلت نسبة الذين أجابوا بأنه موجود 62.7%، وتوافق بشكلٍ تقريبي مع تعرض أفراد العينة للاحتيال عن طريق اليانصيب حيث جاء في المرتبة الثالثة عشر وبلغت نسبة الضحايا 17.2%، أمّا الضحايا من أقارب وأصدقاء أفراد العينة الذين تعرضوا للاحتيال عن طريق اليانصيب في المرتبة الثالثة عشر، وبلغت نسبة الضحايا

18.80%. يتم تفسير هذا النوع من الاحتيال الضحية المولع بالاكتساب، حيث يتم خداع الضحية بأنه بمجرد أن يدفع مبلغًا ماليًّا فإنه سيربح مبلغًا كبيرًا، فلولعه باكتساب المال يقوم بتحويل أموال لهم ظنًّا منه أنه فعلاً ربح مبالغ مالية كبيرة، وأكد ذلك الحالات الآتية: (الحالة الأربعين)، (الحالة الحادية والأربعون)، (الحالة الاثنتان والأربعون) حيث إنهم قاموا بتحويل أموال بسبب خداعهم بربح جائزة عن طريق اليانصيب في الإنترنت.

في المرتبة الحادية عشر جاء الوعي بنوع الاحتيال الإلكتروني عن طريق الشركات، فشكلت نسبة الذين أجابوا بأنه موجود 61.5% وتعارض بشكلٍ تقريبي مع تعرض أفراد العينة للاحتيال الإلكتروني عن طريق الشركات، حيث جاء في المرحلة الثامنة ووصلت نسبة الضحايا إلى 20.74%، أمّا الضحايا من أقارب وأصدقاء أفراد العينة الذين تعرضوا للاحتيال عن طريق الشركات في المرتبة التاسعة، وبلغت نسبة الضحايا 21.25%، فمن خلال وعي أفراد العينة جاء في مرحلة أقل من التعرض، وهذا يشير إلى جهل أفراد العينة بهذا النوع من الاحتيال ممّا سيؤدي إلى زيادته في المستقبل، وأكّد هذا النوع من الاحتيال الحالات الآتية: (الحالة السادسة عشر)، الاحتيال من قبل شركات وهمية لبيع الشقق وعندما قدمت الدفعَة الأولى يتم انسحاب الشركة واختفاؤها نهائيًّا. (الحالة السابعة عشر و الحالة الثامنة عشر)، تم إعطاء رقم البطاقة البنكية لشركة وتم سحب أقصى مبلغ من الحساب، (الحالة التاسعة عشر) الاتصال من شركه تدعي أنها على خبرة طويلة في البورصة وتطلب من العملاء الاشتراك معها، وتدريبهم عبر الهاتف والموقع الخاص بهم مقابل حساب وهمي في بادئ الأمر ثم يطلبون من الضحية تحويل مبلغ من المال، وبعد ذلك يبلغونه أنه تمت خسارة المبلغ في البورصة، وأيضًا تعرض لعملية نصب آخرى من قبل شركة وهمية توعد من يشترك معها بالحصول على الجرين كارد للسفر لأمريكا والعمل والدراسة بها مقابل مبالغ. يتم تفسير هذا النوع من الضحية المتهور: فمن خلال إعطائه بيانات بطاقته

الائتمانية للشركات والوثوق بهم ودفع أموال بدون إبرام العقود القانونية، والتأكد منها فهذا يعتبر سلوكا طائشا كما ظهر في بعض الحالات.

في المرتبة الثانية عشر جاء الوعي بنوع الاحتيال الإلكتروني عن طريق تزوير بطاقة الائتمان، فشكّلت نسبة الذين أجابوا بأنه موجود 57.8%، وتوافق بشكلٍ تقريبي مع تعرض أفراد العينة للاحتيال الإلكتروني عن طريق تزوير بطاقة الائتمان حيث جاء في المرحلة الرابعة عشر، وبلغت نسبة الضحايا 17.2%، وأيضًا الضحايا من أقارب وأصدقاء أفراد العينة الذين تعرضوا للاحتيال عن طريق تزوير بطاقة الائتمان جاء في المرتبة الرابعة عشر حيث وصلت نسبة الضحايا إلى 12.21%، ونتيجة لانخفاض الوعي بهذا النوع من الاحتيال الذي يعود إلى انخفاض التعرض له وربما يزيد في المستقبل يجب التوعية به، ويؤكد هذا النوع من الاحتيال: الحالة السادسة حيث إنه من خلال تقديم للوظيفة عن طريق النت تم استغلال البيانات الشخصية في استخراج بطاقات ائتمان بمساعدة من قبل موظف في البنك. يتم تفسير هذا النوع من خلال الضحية المتهور: فمن خلال إعطائه بياناته الشخصية وبيانات بطاقته الائتمانية لأيّ شخص، وهذا يعتبر سلوكا طائشا من شأنه أن يوقعه ضحية للاحتيال الإلكتروني.

في المرتبة الثالثة عشر جاء الوعي بنوع الاحتيال الإلكتروني عن طريق الاحتيال الإلكتروني عن طريق موظّفي المصارف حيث شكّلت نسبة الذين أجابوا بأنه موجود 55.8%، وتوافق بشكلٍ تقريبي مع تعرض أفراد العينة للاحتيال الإلكتروني عن طريق موظّفي المصارف، حيث جاء في المرتبة الحادية عشر وبلغت نسبة الضحايا 17.91%، وأيضًا الضحايا من أقارب وأصدقاء أفراد العينة الذين تعرضوا للاحتيال عن طريق موظّفي المصارف حيث جاء في المرتبة الحادية عشر ووصلت نسبة الضحايا إلى 19.41%، ونتيجة لانخفاض الوعي بهذا النوع من الاحتيال الذي يعود إلى انخفاض التعرض له، وربما يزيد في المستقبل يجب التوعية به. ويظهر هذا النوع من الاحتيال في الحالة الثالثة: الاحتيال عن طريق موظفي المصارف بأنه سيتم استقطاع مبلغ معين لمدة 20 سنة، فالبنك يستقطع من الشخص بشكلٍ عادي لمدة 5

سنوات ومن بعدها تستقطع مبالغ أخرى يتم الاحتيال بها، ويتم من خلالهم إجبار العميل على دفع المبالغ المالية شهريًّا غير العقد الذي أبرمه أول مرة. ويتم تفسير هذا النوع من الضحية المتهور: فمن خلال توقيع العقود دون التركيز في بنودها بسبب الثقة في البنك أو الموظف، وهذا يعدّ سلوكًا طائشا من شأنه أن يوقعه ضحية للاحتيال الإلكتروني.

في المرتبة الرابعة عشر جاء الوعي بنوع الاحتيال الإلكتروني عن طريق الاحتيال عن طريق سوق العملة الإلكتروني (بيع العملة الافتراضية) شكّلت نسبة الذين أجابوا بأنه موجود 53.2%، وتعارض بين إدراك أفراد العينة والوعي بالاحتيال عبر بيع العملة الافتراضية مع التعرض للاحتيال عبر العملة الافتراضية، حيث جاء في المرحلة التاسعة ووصلت نسبة الضحايا إلى 20.21%، وأمّا الضحايا من أقارب وأصدقاء أفراد العينة الذين تعرضوا للاحتيال عبر سوق العملة الإلكتروني (بيع العملة الافتراضية) جاءت في المرتبة العاشرة وبلغت نسبة الضحايا 20.39%، وتعارض مع وعي أفراد العينة حيث كان في المرحلة الأخيرة، فهذا من شأنه أن يؤدي إلى زيادة ضحايا العملة الافتراضية نتيجة لعدم الوعي بهذا النوع من قبل أفراد المجتمع، الأمر الذي من شأنه أن يؤدي إلى زيادته مستقبلاً، ويؤكد هذا النوع من الاحتيال (الحالة الأولى)، (الحالة الثانية) حيث إنه تم خداعهم من خلال البتكوين أنهم سيربحون مبالغ، وبعد دخولهم وإيداعهم لأموالهم سرعان ما يخسرون كامل المبلغ. ويتّضح هذا في شخصية الضحية المولع بالاكتساب حيث يتم خداع الضحية بأنه سيكسب أرباحًا كبيرة، وأنه سيتم مضاعفة أمواله.

هل يختلف تعرض أفراد العينة للاحتيال الإلكتروني حسب كل من متغيرات: (الجنس، والعمر، والمستوى التعليمي، والجنسية)؟

تبيّن من خلال نتائج الدراسة في التعرف على العلاقة بين الجنس، والعمر، والمستوى التعليمي، والجنسية أنه ليس هناك علاقة ذات دلالة إحصائية بين التعرض

للاحتيال الإلكتروني وبين العمر والجنس والجنسية فجميعهم يتعرضون للاحتيال الإلكتروني بنفس المستوى، فاختلفت مع نتائج دراسة (المطيري، 2008م) حيث أشارت الدراسة إلى أن الذين تتراوح أعمارهم ما بين (36–45) أكثر الفئات تعرّضًا للاحتيال، ودراسة (هلال، 2012م) أن أغلب ضحايا جرائم السرقة أعمارهم من 35–50 فتعارضت الدراسة مع الدراستين، حيث إنّ أيّ فرد مهما كان عمره أو جنسه أو جنسيته يمكن أن يتعرض لأحد أنواع الاحتيال، فمع اندماج الناس بوسائل التواصل الاجتماعي أصبح العمر غير محدد فجميع الفئات العمرية والجنسيات والذكور والإناث يخوضون تجارب السوشال ميديا، ويتعرضون للاحتيال عن طريقه، أما بالنسبة للمستوى التعليمي فكان هناك علاقة ذات دلالة إحصائية بين المستوى التعليمي والتعرض للاحتيال الإلكتروني، ويعود ذلك إلى أن للمستوى التعليمي تأثير إيجابي في التعرض للاحتيال الإلكتروني، فنتيجة للوعي المسبق فلن يتعرض الشخص للاحتيال الإلكتروني، وأثناء مقابلة رجال القانون من شرطة أو قضاة أو محاميين لم يتعرضوا للاحتيال الإلكتروني نتيجة لوعيهم المسبق بهذه الأنواع، فالتعليم والتوعية لهم دور فعّال في التقليل من الاحتيال الإلكتروني. وفي الدراسة يتّضح أنّ عددًا كبيرًا من مستوى البكالوريوس تعرضوا للاحتيال، ولكن بالنظر للعدد الإجمالي يلاحظ أنهم يمثلون غالبية العينة، ولكن بالنظر للمستويات التعليمية الأخرى يلاحظ أن معظمهم تعرضوا للاحتيال الإلكتروني، واتفقت هذه الدراسة مع نتائج دراسة (المطيري، 2008م) .

أشارت نتائج الدراسة إلى أنه ليس هناك علاقة ذات دلالة إحصائية بين التعرض للاحتيال الإلكتروني عبر بيع العملة الافتراضية وبين العمر والجنس والجنسية والمستوى التعليمي فجميعهم يتعرضون للاحتيال الإلكتروني بنفس المستوى بسبب انتشار المعلنين لمثل هذه التجارة، والذين يقومون بخداع الناس من خلالها وإيهامهم بالربح المالي الكبير، وتناول هذا الجانب الضحية المولع بالاكتساب حيث إنّ جميع شرائح المجتمع يتعرضون لمثل هذا النوع من الاحتيال باختلاف أعمارهم وجنسياتهم

وجنسهم ومستواهم التعليمي، وبخاصة أنه يعتبر نوعًا من التجارة الحديثة التي يرغب الإنسان في تجربتها من واقع حب الفضول، وتفسّر ذلك نظرية أنماط الحياة، فمن خلال نمط حياة الإنسان ورغبته في تجربة كلّ شي، والمكون العقلاني الذي يجعله يتّخذ القرارات، فيجعله يميل إلى الرغبة في التجربة مع وجود جاذبية الهدف الذي يتمثّل في الربح العالي الذي يوهمونهم به فيتم خداع الضحايا وجعلهم يخوضون هذه التجارب. وأكدت الحالات الآتية ذلك (الحالة الأولى)، (الحالة الثانية) حيث إنهما من جنسيتين مختلفتين ولكن أعمارهم متقاربة، مع وجود أعمار مختلفة وأحدهما ذكر والآخر أنثى، وهذا دلالة على أن جميع الأفراد يتعرضون للاحتيال الإلكتروني عبر بيع العملة الافتراضية في المستوى نفسه.

وأشارت نتائج الدراسة إلى عدم وجود علاقة ذات دلالة إحصائية بين الجنس والعمر والجنسية والمستوى التعليمي والتعرض للاحتيال الإلكتروني عن طريق موظّفي المصارف، فمع الرغبة في إنجاز المعاملات أصبح الأفراد يقومون بإبرام العقود دون النظر في بنودها، الأمر الذي أدّى إلى زيادة الاحتيال الإلكتروني وانتشاره أكثر من السابق، وأكد ذلك (الحالة الثالثة)، ويتمثّل في الشخصية المتهور الذي يقدم على الفعل دون التأكد منه، ممّا يؤدّي للاحتيال عليه، وفسّرت ذلك نظرية نمط الحياة، فنمط الحياة القائم على السرعة في حياة غالبية الشعب تجعلهم يقومون بالتوقيع على أيّ عقد دون النظر في بنوده، ومن خلال نظرية النوافذ المحطّمة، فما يقوم به الفرد من توقيع للعقد دون قراءة بنوده يعطي للجاني ثغرة للاحتيال عليه من خلال بند من بنود العقد.

ودلّت النتائج على أنّ هناك علاقة ذات دلالة إحصائية بين العمر والجنسية والجنس والمستوى التعليمي والتعرّض للاحتيال الإلكتروني عن طريق الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان، حيث إنّه لا تتأثر الجنسية أو الجنس أو المستوى التعليمي والفئات العمرية في التعرض لهذا النوع من الاحتيال، وذلك بسبب زيادة استخدام كافة الفئات العمرية لبطاقة الائتمان في شبكة الإنترنت، واندماجهم في

الإنترنت، وإنّ الذكور والإناث يتعرضون للاحتيال بالمستوى نفسه، وأكّدت ذلك (الحالة الرابعة) أنثى، وتتمثّل في الضحية المولعة بالاكتساب، فأعطتهم الرقم السري ظنًّا منها أنهم سيقومون بتحويل مبلغ مالي لها، و(الحالة الخامسة) ذكر، وتمثل بالضحية المتهورة، حيث إنه من خلال وضعه لبيانات بطاقته الائتمانية في موقع إلكتروني ودفع أموال قبل استلام البضاعة، وهذا يعتبر سلوكًا طائشًا. وجميع الجنسيات والمستويات التعليمية يتعرضون لهذا النوع من الاحتيال، وتؤكد التعرض لهذا النوع من الاحتيال نظرية النوافذ المحطمة، فبوضع بيانات بطاقة الائتمان في الموقع الإلكتروني يجعل ثغرة للجاني لسرقته والاستيلاء على أمواله، ونظرية أسلوب الحياة من خلال المكوّن العقلاني، حيث إنّ الهدف يتمثل في بطاقة الائتمان والمبلغ الكبير فيتخذ قرارًا لسرقته.

ودلّت النتائج أنه ليس هناك علاقة ذات دلالة إحصائية بين العمر والجنسية والجنس والمستوى التعليمي والتعرض للاحتيال الإلكتروني عن طريق تزوير بطاقة الائتمان لأنه يتم استغلال بيانات أيّ شخص بغض النظر عن عمره أو جنسيته أو جنسه أو المستوى التعليمي له، فبإعطاء البيانات لأيّ شخص كما حدث في (الحالة السادسة)، حيث إنه أعطى بيانات خاصة لشخص بغرض التوظيف فاستغلّها واستخرج بطاقة باسمه وتمثّل في الشخصية المتهورة، حيث إنّه أعطى بياناته دون التأكّد من صدق الشخص، ونظرية أسلوب الحياة من خلال المكون العقلاني حيث إنّ الهدف يتمثّل في بطاقة الائتمان، وتوفر البيانات لديه، والتي يمكن استغلالها في غياب صاحبها واستخراج بطاقة أخرى.

دلّت النتائج أنه ليس هناك علاقة ذات دلالة إحصائية بين العمر والجنسية والجنس والمستوى التعليمي والتعرض للاحتيال الإلكتروني التجاري، حيث إنّ أيّ شخص بغض النظر عن عمره أو جنسيته أو جنسه أو المستوى التعليمي يقوم بالتسوّق الإلكتروني يكون عرضة للاحتيال الإلكتروني التجاري، وأكّد ذلك الحالات الآتية (الحالة الثامنة)، (الحالة التاسعة)، (الحالة العاشرة)، (الحالة الحادية عشر)، (الحالة الثانية عشر)، (الحالة الثالثة عشر)، (الحالة الرابعة عشر)، (الحالة الخامسة عشر)

فاختلفت جنسياتهم وأعمارهم وأجناسهم ومستواهم التعليمي، ويتمثّلون بالشخصية المتهوّرة فمن خلال وضعه لبيانات بطاقته الائتمانية في أيّ موقع ودفع أموال قبل استلام البضاعة، ولا سيما إذا كانت بضائع باهضة الثمن. كما ظهر في بعض الحالات، وهذا يعتبر سلوكًا طائشًا، فكيف يقوم بالدفع قبل أن يستلم البضاعة ويفحصها جيدًا، وبخاصة إذا كانت سيارة كما ذكرت الحالتين: (الحالة العاشرة) و(الحالة التاسعة). ومن خلال أسلوب حياة الفرد بوضعه لبياناته الشخصية واستمراره بالدفع قبل الاستلام في جميع المعاملات، وتسوّقه لجميع احتياجاته من الإنترنت؛ كشراء بضائع باهضة الثمن مثل خاتم ألماس أو سيارات أو أراضٍ أو شقق دون التأكد منها، والدفع قبل الاستلام هذا من شأنه أنه يوقعه كضحية للاحتيال الإلكتروني.

دلّت النتائج على وجود علاقة بين العمر والجنس والتعرض للاحتيال عن طريق الشركات حيث أظهرت الدراسة أنه يختلف التعرض للاحتيال عن طريق الشركات باختلاف الجنس والعمر، واتفقت مع دراسة هلال (2005م)، وليس هناك علاقة ذات دلالة إحصائية بين المستوى التعليمي والجنسية والتعرّض للاحتيال الإلكتروني عن طريق الشركات الضحية المتهور: فمن خلال إعطائه بيانات بطاقته الائتمانية للشركات والوثوق بهم، ودفع أموال دون إبرام العقود القانونية، والتأكد منها، وهذا يعتبر سلوكًا طائشًا كما ظهر في بعض الحالات، مثل: (الحالة السادسة عشر)، و(الحالة السابعة عشر)، و(الحالة الثامنة عشر)، و(الحالة التاسعة عشر).

وأشارت النتائج إلى أنه ليس هناك علاقة ذات دلالة إحصائية بين العمر والجنس والجنسية والمستوى التعليمي والتعرض للاحتيال الإلكتروني عن طريق المحافظ الاستثمارية الوهمية الإلكترونية، حيث يتم خداع جميع الأفراد بالربح الشهري العالي؛ مثل أن يقال ادفع 100000 وسيكون لك ربح شهري 10 آلاف، فيتم إعطاؤه لعدد من الأشهر إلى أن يثق بهم، ويقول لأصدقائه وأقاربه وتتضاعف عندهم المبالغ، وبعد ذلك يقولون إنهم أفلسوا، ويهربون بأموال الضحايا. ويتمثلون بالضحية المولع بالاكتساب حيث يتم خداع الضحية بأنه سيكسب أرباح كبيرة، وأنه سيتم مضاعفة

أمواله، وأكّد ذلك الحالات الآتية (الحالة السادسة والعشرين)، (الحالة السابعة والعشرين).

وأشارت النتائج أنه ليس هناك علاقة ذات دلالة إحصائية بين العمر والجنس والمستوى التعليمي والجنسية والتعرض للاحتيال عن طريق الإعلان عن الوظائف الوهمية، حيث إنّ جميع الأفراد يبحثون عن وظائف سواء ذكورًا أم إناثًا، وباختلاف مراحلهم العمرية ومستوياتهم التعليمية وباختلاف الجنسية، ويتم استغلالهم من بعض الشركات بالإعلان عن وظائف وتركهم يعملون دون توقيع عقد، وبعد ذلك لا يعطونهم النقود، كما حدث مع (الحالة الثامنة والعشرين) حيث تركوها تعمل وبعد الانتهاء تبين لها أنه تم خداعها، ويتم تفسير ما حدث معها بالضحية المولع بالاكتساب، فهنا الضحية يرغب في العمل وكسب الرزق، ويقوم بأيّ عمل دون التأكد منه ومن دون أيّ إثبات، فيتم خداعه.

أشارت النتائج إلى أن هناك علاقة ذات دلالة إحصائية بين المستوى التعليمي والتعرض للاحتيال الإلكتروني عن طريق انتحال صفة كبار، وليس هناك علاقة ذات دلالة إحصائية بين العمر والجنس والجنسية والتعرض للاحتيال الإلكتروني عن طريق انتحال صفة كبار الشخصيات، فنتيجة لوعي أفراد العينة وارتفاع المستوى التعليمي يكونون على وعي بأن الشيوخ لن يقوموا بطلب أموال منهم، ويتم غالبًا خداع الفئات ذات التعليم المنخفض، أمّا العمر والجنس والجنسية فليس لها علاقة في التعرض للاحتيال عبر انتحال صفة كبار الشخصيات وجميعهم يتعرضون بنفس المستوى، وأكّد ذلك (الحالة التاسعة والعشرين)، حيث أكّد أنه تعرّض للنصب عن طريق شخصية انتحلت شخصية أحد بنات الحكام وقام بالتحويل لها، وهذا يعتبر ضحية مسهلاً، لأنه تواصل مع الضحية بشكلٍ شخصي وقام بالتحويل دون التأكّد، ودخل لبيئة لا يعرفها وغير متأكد منها.

وبيّنت الدارسة وجود علاقة ذات دلالة إحصائية بين الجنس والجنسية والعمر والتعرض للاحتيال الإلكتروني عن طريق التسول الإلكتروني، حيث كان عدد الذكور

82 أما الإناث 87، ولكن بالعودة لعدد الذكور من أفراد العينة وعدد الإناث يظهر أن عدد الذكور أكثر عرضة من الإناث لأنه يتم استغلالهم من قبل النساء، ويتم خداعهم وإظهار فقرهم، كما أكّدت الحالة الحادية والثلاثين، وأمّا الجنسية فالجنسية الإماراتية أكثر تعرّضًا للاحتيال عبر التسوّل الإلكتروني بسبب حب الخير لدى الشعب الإماراتي وعدم وعيهم بأنّ هؤلاء عصابة تقوم بالنصب على أبناء الخليج، فتأتي غالبًا امرأة وتقول إنها لا تجد قوت يومها هي وأطفالها، فتثير استعطاف الشعب ممّا يؤدّي إلى أن يقوموا بالتحويل لها، وأيضًا يتعرّضون للنساء نظرًا لرؤيتهم صورًا للأطفال الذين ترسلهم هذه العصابة على أنهم أطفالهم وجائعون، ولأنّ المرأة عاطفية جدًا تتأثر وتقوم بتصديقهم وتحوّل مبالغ لهم، وأكّدت ذلك الحالة الثلاثين وضحايا الاحتيال عن طريق التسول الإلكتروني، ويتمثلون بالضحية المسهل لأنه قد قام بالتواصل مع الضحية وأعطاه كل ما يريده دون أن يتأكد، وليس هناك علاقة ذات دلالة إحصائية بين المستوى التعليمي والتعرض للاحتيال الإلكتروني عن طريق التسول الإلكتروني لأنّ جميع المستويات التعليمية من الممكن أن تنخدع بالصور التي تقوم بإرسالها هذه العصابات.

وأثبتت الدراسة أنه ليس هناك علاقة ذات دلالة إحصائية بين الجنس والعمر والمستوى التعليمي والجنسية والتعرض للاحتيال الإلكتروني العاطفي، حيث إنّ الناس باختلاف المستويات التعليمية يتعرضون للاحتيال العاطفي، وسواء كانوا ذكورًا أم إناثًا وبمختلف الفئات العمرية فالمسنّ يتعرّض –والمراهق والذي هو أقل من 18 وبمختلف الجنسيات– للاحتيال العاطفي. ويفسر هذا النوع من الاحتيال الضحية المسهل، فالضحية هنا قد تواصل مع الجاني وأعطاه كلّ البيانات الكافية لاستغلالها ضده، وأكّد ذلك الحالات الآتية: (الحالة العشرون)، (الحالة الحادية والعشرون)،(الحالة الثانية والعشرون)، (الحالة الثالثه والعشرون)، الحالة الرابعة والعشرون)، (الحالة الخامسة والعشرون) حيث إنهم جميعًا تعرضوا للاحتيال الإلكتروني نتيجة لإعطائهم البيانات وتواصلهم مع الجناة.

وأثبتت الدراسة أن ليس هناك علاقة ذات دلالة إحصائية بين العمر والجنس والجنسية والمستوى التعليمي والتعرض للاحتيال والنصب عبر الهاتف، حيث إنّ الناس باختلاف المستويات التعليمية يتعرضون للاحتيال عبر الهاتف، وسواء كانوا ذكورًا أم إناثًا وبمختلف الجنسيات والأعمار لأنهم يتواصلون مع كافة أفراد المجتمع، ويؤكد هذا النوع من الاحتيال الحالات الآتية: (الحالة الثانية والثلاثون)،(الحالة الثالثة والثلاثون)، (الحالة الرابعة والثلاثون)، (الحالة الخامسة والثلاثون)، ويفسّر هذا النوع من الاحتيال الضحية المولع بالاكتساب فيتم خداع الضحية بأنه ربح مبلغًا ماليًّا وليتم تحويلها يجب أن يرسل مبلغًا نقديًّا لهم، فلولعه باكتساب المال يقوم بتحويل أموال لهم ظنًّا منه أنه فعلاً ربح مبالغ مالية كبيرة.

وأثبتت نتائج الدراسة عدم وجود علاقة ذات دلالة إحصائية بين العمر والمستوى التعليمي والجنسية والتعرض للاحتيال عبر وسائل التواصل الاجتماعي، وهناك علاقة ذات دلالة إحصائية بين الجنس والتعرض للاحتيال عبر وسائل التواصل الاجتماعي؛ أي: أنّ هناك علاقة، حيث إنّ الناس باختلاف أعمارهم ومستوياتهم التعليمية وجنسياتهم يتعرضون للاحتيال عبر وسائل التواصل الاجتماعي، ولكن يتأثر الجنس في تعرضهم لهذا النوع لأن الإناث أكثر استخدامًا لوسائل التواصل الاجتماعي وأكثر ثقة بالبشر. وتتمثل بالضحية المسهل، فقد قام بالتواصل مع الضحية وأعطاه البيانات التي تسهّل اختراق جهازه. وتمثّل في (الحالة السادسة والثلاثين)، (الحالة السابعة والثلاثين)، (الحالة الثامنة والثلاثين)، (الحالة التاسعة والثلاثين)، ويؤكّد ذلك نظرية النوافذ المحطمة حيث إنه من خلال نظرية النوافذ المحطمة التي تقوم على فكرة الإهمال الذي يؤدي إلى خلق الظروف المناسبة للجريمة، فالنافذة المحطمة تعدّ ثغرة لدخول الجاني: فمن خلال الاستخدام الزائد لوسائل التواصل الاجتماعي، وفتح أيّ رابط يصل للشخص ويتواصل مع أيّ شخص، وهذا من شأنه أن يؤدّي إلى سهولة اختراق هاتف هذا الشخص، والتوصل إلى أصدقائه والاحتيال عليهم وطلب المال، وأيضًا أكّدت نظرية نمط الحياة أن لوسائل التواصل الاجتماعي دور في التعرض للاحتيال من خلال

التوصل إلى أن أنماط النشاطات أو نمـــط الحياة للأفراد يعرضهم بدرجات متفاوتة لاحتمالية أن يكونوا ضحايا محتملين، وكان جوابهم هو أن النشاطات المنمطة، أو أنماط حياة الأفراد، تقود إلى معدلات ضحايا مختلفة. وتمتاز أنماط الحياة هذه بأنها وظائف يومية تشمل نشاطات العمل ونشاطات أوقات الفراغ فمن خلال قضاء وقت الفراغ لساعات طويلة على الإنترنت والتواصل مع العديد من الناس المختلفين الأمر الذين يجعله عرضه للاحتيال الإلكتروني.

ودلّت النتائج أنه ليس هناك علاقة ذات دلالة إحصائية بين الجنس والجنسية والمستوى التعليمي والعمر والتعرض للاحتيال عبر اليانصيب، حيث إنه الناس باختلاف أجناسهم وأعمارهم ومستوياتهم التعليمية وجنسياتهم يتعرضون للاحتيال عبر اليانصيب لأنهم يتواصلون مع كافة أفراد المجتمع، ويؤكد هذا النوع من الاحتيال الحالات الآتية: (الحالة الأربعون)، (الحالة الحادية والأربعون)، (الحالة الاثنتان والأربعون)، ويفسر هذا النوع من الاحتيال الضحية المولع بالاكتساب، فيتم خداع الضحية بأنه ربح مبلغًا ماليًّا في اليانصيب، وليتم تحويلها يجب أن يرسل مبلغًا نقديًّا لهم، فلولعه باكتساب المال يقوم بتحويل أموال لهم ظنًّا منه أنه فعلاً ربح مبالغ مالية كبيرة.

هل لاستخدام برامج التواصل الاجتماعي والتسوق الإلكتروني دور في التعرض للاحتيال الإلكتروني؟

أثبتت الدراسة وجود علاقة ضعيفة ذات دلالة إحصائية بين التعرّض للاحتيال الإلكتروني وبين وسائل التواصل الاجتماعي المستخدمة، حيث إنه مع زيادة الجلوس واستخدام برامج التواصل الاجتماعي لساعات طويلة هذا من شأنه أن يجعل الفرد يتواصل مع الغرباء بكثرة مما يؤدي إلى زيادة احتمالية وقوعه كضحية للاحتيال الإلكتروني، وأكد ذلك دراسة (العنزي، 2016م) من خلال سهولة التواصل بين الجنسين عبر الوسائل التقنية المختلفة، ما ينتج عنه في الأخير اعتداء على حرمة

الحياة الخاصة للفرد عن طريق الحصول على معلومات تخصّ المجني عليه وتكون سلاحًا بيد المبتز يســــلطه على الضحية كلما أراد تحقيق نتيجة لصالحه. وأكد ذلك الحالات الآتية: (الحالة العشرون)، (الحالة الحادية والعشرون)، (الحالة الثالثة والثلاثون)، (الحالة الرابعة والثلاثون)، (الحالة الرابعة والعشرون)، (الحالة الخامسة والعشرون)، حيث تؤكد هذه الحالات علاقة وسائل التواصل الاجتماعي بالتعرض للاحتيال الإلكتروني، فمن خلال التواصل الاجتماعي مع الغرباء من خلال هؤلاء الحالات أدى إلى الاحتيال عليهم والإيقاع بهم ضحايا للاحيال الإلكتروني. وتؤكّد ذلك نظرية النوافذ المحطمة: والتي تقوم على فكرة الإهمال، والذي يؤدي إلى خلق الظروف المناسبة للجريمة، فالنافذة المحطمة تعدّ ثغرة لدخول الجاني: فمن خلال الاستخدام الزائد لوسائل التواصل الاجتماعي ومشاركة البيانات مع جميع الناس يصبح الشخص عرضه لأن يكون ضحية، فمن خلال إهماله لبياناته ونشرها على برامج التواصل يسمح لأي شخص باستغلالها وارتكاب أنواع الجرائم في الشخص من خلالها مثل النافذة المحطمة التي تسمح لأيّ شخص بالدخول للمنزل من خلالها وسرقته.

وأكّدت نظرية نمط الحياة أنّ لوسائل التواصل الاجتماعي دور في التعرض للاحتيال من خلال التوصّل إلى أن أنماط النشاطات أو نمــط الحياة للأفراد يعرّضهم بدرجات متفاوتة لاحتمالية أن يكونوا ضحايا محتملين، وكان جوابهم هو أن النشاطات المنمطة، أو أنماط حياة الأفراد، تقود إلى معدلات ضحايا مختلفة، وتمتاز أنماط الحياة هذه بأنها وظائف يومية تشمل نشاطات العمل ونشاطات أوقات الفراغ، فمن خلال قضاء وقت الفراغ لساعات طويلة على الإنترنت والتواصل مع العديد من الناس المختلفين، الأمر الذين يجعله عرضه للاحتيال الإلكتروني، ونصنّف الضحية الذي يتعرّض للاحتيال الإلكتروني من خلال التواصل الإلكتروني بالضحية المسهل لأنه يقوم بالتواصل مع الجاني ويعطيه البيانات التي تؤدي إلى الاحتيال عليه من خلالها.

وأثبتت الدراسة وجود علاقة ذات دلالة إحصائية بين التسوق الإلكتروني والتعرض للاحتيال الإلكتروني، وأكّدت تفضيل أفراد العينة للدفع عند الاستلام في

حال التسوق الإلكتروني بسبب خوفهم من الوقوع ضحية لسرقة بيانات بطاقة الائتمان أو خوفهم من عدم وصول البضاعة أو عدم مطابقتها للمواصفات المعروضة، وهذا يعني أن أفراد العينة على وعي بأنّ التسوق الإلكتروني له علاقة بتعرضهم للاحتيال الإلكتروني، وبخاصة إذا لم يتم الحذر في استخدامه. وأكّد هذا الحالات الآتية: (الحالة الثامنة)، (الحالة التاسعة)، (الحالة العاشرة)، (الحالة الحادية عشر)، (الحالة الثانية عشر)، (الحالة الثالثة عشر)، (الحالة الرابعة عشر)، (الحالة الخامسة عشر) فجميعهم تعرّضوا لأنواع الاحتيال بمستويات مختلفة نتيجة للتسوق الإلكتروني، ويظهر هذا من خلال الضحية المتهوّر: فمن خلال وضعه لبيانات بطاقته الائتمانية في أيّ موقع ودفع أموال قبل استلام البضاعة ولا سيما إذا كانت بضائع باهضة الثمن، كما ظهر في بعض الحالات، فهذا يعتبر سلوكًا طائشًا.

ما هو دور أفراد العينة في تعرضهم للاحتيال الإلكتروني؟

أشارت نتائج الدراسة إلى أنّ للضحية دور في التعرض للاحتيال الإلكتروني، ويتّضح ذلك من خلال ارتفاع عوامل الموافقة من أفراد العينة على أن للضحية دور في تعرضه للاحتيال الإلكتروني، فجاء العامل الأول على أن عدم الوعي بأساليب الاحتيال الإلكتروني يزيد من جرائم الاحتيال الإلكتروني بنسبة 92.9%، بينما أفادت الدراسة أنّ معظم أفراد العينة على معرفة بوجود أنواع الاحتيال وربما يعود ذلك إلى معرفتهم بها بعد تعرضهم للاحتيال، وجهلهم في السابق بأنواع الاحتيال ما أدّى إلى تعرّضهم للاحتيال الإلكتروني، واتّفقت هذه النتيجة مع جميع الحالات التي تعرّضت للاحتيال، حيث إنّ نتيجة عدم وعيهم بالاحتيال الإلكتروني أدّى إلى وقوعهم ضحية للاحتيال الإلكتروني واتفقت هذه النتيجة مع دراسة (شوال، 2008م) حيث توصلت إلى أن الجهل بالمحيط الاجتماعي يزيد من احتمالية وقوع الشخص ضحية للجريمة بمتوسط (3.64)، يليه الجهل بالتدابير الأمنية لدى المستهلك (الحيطة والحذر من الوقوع ضحية للاحتيال الإلكتروني)، فنتيجة لعدم الوعي بالأساليب الأمنية التي تحمي

الضحية يؤدي هذا إلى وقوعه ضحية للاحتيال الإلكتروني، ويظهر هذا في الضحية المتهور الذي يقوم بسلوكيات طائشة تؤدي به إلى الوقوع ضحية للاحتيال الإلكتروني، ويليه إهمال الضحايا في التعامل مع بياناتهم الشخصية، واتفقت النتيجة مع الحكيم (2007م) لإهمال ضحايا السرقات في المحافظة على ممتلكاتهم دور في وقوعهم ضحية لجريمة السرقة، واتفقت مع دراسة شوال (2008م) أن إهمال بعض الضحايا في التعامل مع ممتلكاتهم أدّى إلى سرقتها بمتوسط حسابي (3.62)، ويتمثّل في الضحية المهمل، فالضحية هنا يغفـل اتّخـاذ احتيـاط يوجبـه الحذر وتمليه الخبرة الإنسانية على من كان في مثل ظروفـه، فنتيجة لتركه بياناته وعدم الحذر يؤدّي إلى الوقوع ضحية للاحتيال، ويليه عدم إبلاغ الضحايا عن تعرّضهم للاحتيال الإلكتروني بنسبة 88.6%، فنتيجة لعدم الإبلاغ يشعر المجرمون بالأمان، الأمر الذي يجعلهم يزيدون من جرائمهم، واتفقت مع دراسة شوال (2008م) حيث توصّلت الدراسة إلى أن عدم تعاون بعض الناس في الإبلاغ عن المجرمين يؤدي إلى زيادة أعداد الضحايا بمتوسط حسابي (3.56) يليه الثقه الزائدة لدى المستهلك (الدفع قبل الاستلام) بنسبة 87%، وأكّدت على العوامل نظرية النوافذ المحطمة التي تقوم على فكرة الإهمال الذي يؤدي إلى خلق الظروف المناسبة للجريمة، فتفسر النظرية إهمال الضحايا في التعامل مع بياناتهم الشخصية والجهل بالتدابير الأمنية لدى المستهلك والثقه الزائدة لديه، كل هذه العوامل تؤدي إلى تعرضه للاحتيال الإلكتروني، فنتيجة إهمال الضحايا لممتلكاتهم وبياناتهم والثقه الزائدة لدى الآخرين أعطى للجاني ثغرة للوصول إلى بيانات وممتلكات المجني عليه واستغلالها ضده ومصطلح النوافذ المحطمة ينصّ على أنه مثلما تركت نافذة مكسورة بدون دلالة، فهذا سيجعل المارة يظنون أن لا أحد يهتم ممّا سيؤدي إلى تحطيم مزيد من النوافذ، وهذا يفسر أنه في حال عدم الإبلاغ عن الجرائم وعدم اتخاذ الإجراءات المناسبة هذا من شأنه أن يؤدي إلى انتشار الجرائم ووعي المجرمين بعدم جرأة الضحايا على الإبلاغ، وأكّدت ذلك نظرية نمط الحياة: والتي تقوم على معرفة الأسباب التي تضع بعض الجماعات تحت الخطورة وليكونوا ضحايا للجريمة دون

غيرهم؛ أي: ما هي الأنشطة التي يقومون بها وتجعلهم عرضه لأن يكونوا ضحايا للجريمة، ولقد توصلوا إلى أن أنماط النشاطات أو نمــط الحياة للأفراد يعرّضهم بدرجات متفاوتة لاحتمالية أن يكونوا ضحايا محتملين من خلال نشاطاتهم وقضاء أوقات فراغهم على الإنترنت وتعرفهم على العديد من الأشخاص وثقتهم الزائدة بهم ومشاركة بياناتهم الشخصية معهم دون الوعي بالمحيط الاجتماعي وأساليب الاحتيال الإلكتروني الشائعة، واعتمادهم إنجاز كافة معاملاتهم على الإنترنت، ومن مبدء الثقة بالأصدقاء الافتراضيين بأسلوب غير عقلاني، الأمر الذي من الممكن أن يؤدي إلى أن يتم استغلالهم والاحتيال عليهم، فمن خلال هذه الأنماط الحياتية تزيد احتمالية الوقوع ضحية للاحتيال الإلكتروني.

هل يقوم أفراد العينة بالإبلاغ عند تعرضهم للاحتيال، وما الأسباب التي تحول دون إبلاغهم؟ وهل هم على دراية بالقوانين التي تكفل حقّهم في حال تعرّضهم للاحتيال الإلكتروني؟

أشارت نتائج الدراسة أنّ معظم الذين تعرضوا للاحتيال لإلكتروني لم يبلغوا، وذلك بنسبة 19.7%، ومن ضمن حالات الذين لم يقوموا بالإبلاغ: الحالة الأولى، الحالة الخامسة عشر، الحالة الثامنة عشر، الحالة الحادية والعشرون، الحالة الثالثة والعشرون، الحالة الخامسة والثلاثون حيث تعرضوا لأنواع احتيال مختلفة لكنهم لم يقوموا بالإبلاغ ظنًّا منهم أنّ القانون لن يحميهم وبسبب الخوف من سخرية الآخرين، بعد ذلك جاءت نسبة الذين أبلغوا الشرطة بنسبة 12.3% بعد ذلك الأسرة بنسبة 9.9%، ويليه من قاموا بإبلاغ الأسرة والأصدقاء 9.5%، ثم جاءت نسبة الذين أبلغوا الأصدقاء فقط بنسبة 5.4%، يليه الذين أبلغوا الأسرة والأصدقاء بنسبة 2.2%، ثم الذين أبلغوا البنك فقط بنسبة 2.1%، ثم الذين أبلغوا الأصدقاء والشرطة بنسبة 1.1%، ثم اشتركوا الاتصالات أو دو مع الذين أبلغوا البنك والشرطة مع الذين أبلغوا حماية المستهلك بنسبة 0.3%، يليه السفارة 0.1%، وأخيرًا كلّ ما سبق 5.6%، وجاء أعلى سبب وراء عدم إبلاغهم هو قناعتهم بأن القانون لا يحمي ضحايا الاحتيال الإلكتروني

بعدد 237 أو كما كان يقال أثناء المقابلات القانون لا يحمي المغفلين، ولكن في الوقت ذاته معظم أفراد العينة على جهل بالمواد القانونية التي تتعلق بالاحتيال الإلكتروني في مرسوم مكافحة جرائم تقنية المعلومات، حيث كانت نسبتهم 26.1% فقط على معرفة بالقانون، وأن هناك قانونًا يحمي ضحايا جرائم تقنية المعلومات في حين أن 73.9% أجابوا أنهم لم يطلعوا على القانون، وبعضهم قد قال أثناء المقابلات إنه لا يعلم بوجود هذا القانون. إذا أجاب أفراد العينة أنهم لم يبلغوا بسبب عدم قناعتهم بأن القانون يحمي ضحايا الاحتيال في الوقت الذي هم لم يقوموا فيه بالاطلاع على القانون ويجهلونه إذا كانوا غير مقتنعين بالقانون إنما هم جاهلون به.

أمّا بالنسبة للقانون فارتفعت موافقة أفراد العينة على أن عدم تعاون الضحايا في الإبلاغ عن عمليات الاحتيال الإلكتروني أدى إلى زيادتها بعدد 418، وهذا دليل على أن عدم إبلاغ الضحايا يعطي مجال للجناة للتمادي في ارتكاب المزيد من الجرائم في حق ضحايا آخرين، واتفقت مع الدراسة الشوال (2008م) يليه: هل تعتقد أن هناك قواعد وتشريعات تحمي ضحايا الاحتيال الإلكتروني؟ وأجاب 395 بنعم، فالمتابع للقانون يلاحظ وجود تشريعات وقوانين كثيرة تحمي ضحايا الاحتيال الإلكتروني ولكن معظم أفراد المجتمع يجهلونه، يليه: هل تعتقد أن القانون يحمي ضحايا الاحتيال الإلكتروني؟ أجاب 396 بنعم، بعد ذلك عدم تناسب العقوبة التي توقع على الجناة أدّى إلى عدم الإبلاغ عن جرائم الاحتيال الإلكتروني وأجاب بنعم 273، أخيرًا السؤال الذي وجهه للضحايا وأقاربهم بعد تعرضك للاحتيال الإلكتروني هل أوجد القانون طريقة تكفل حقك؟ أجابوا بنعم 255، وأجاب بلا 69 في حين أجاب 154 بلا أعلم، وهم الذين لا يعلمون إذا تم أخذ حق أقاربهم وأصدقائهم أو لم يتم الانتهاء من قضيتهم وبعدهم لم يتعرضوا، وأثبتت الحالات الآتية أن بعد تعرضهم للاحتيال وإبلاغهم لم يتم أخذ حقهم الحالة الثانية، الحالة الرابعه، الحالة التاسعة، الحالة الحادية عشر، الحالة السابعة عشر، الحالة الثالثة والثلاثون، الحالة الثانية والثلاثون. وتشير الحالات التي لم يتم أخذ حقها أنه بسبب عدم وجود إثبات أو أن الجاني خارج الدولة. وقد أشارت

دراسة الزهراني، (2014م) إلى أنه لم يتناول النظام السعودي أو القانون الإماراتي وسائل الإثبات التي يمكن الاعتماد عليها في إثبات جريمة الاحتيال الإلكتروني. وكشفت نتائج الدراسة أنه لم يحدد النظام السعودي أو القانون الإماراتي سبل التنسيق مع الدول الآخرى، وهذا يعني صعوبة الوصول للجاني إذا كان من دولة آخرى، وهذا يزيد من جرائم الاحتيال الإلكتروني. وتؤكّد نظرية النوافذ المحطمة أنّه في حال تركت نافذة مكسورة بدون دلالة فهذا سيجعل المارة يظنون أن لا أحد يهتم ممّا سيؤدي إلى تحطيم مزيد من النوافذ، وانتشار الفوضى. وهذا يدل على أنه في حال قيام المحتال بالاحتيال على الضحية وعدم إبلاغ الضحية وعدم اتخاذ أيّ إجراء ضده سيظن أن الأمر عادي، ممّا يجعله يستمر في عمليات الاحتيال الإلكتروني، ممّا يؤدّي إلى انتشارها.

الخاتمة

التوصيات

1. التدخّل التشريعي لمواجهة القصور في التشريعات والقوانين الجزائية أو تحديثها بالنص صراحة على تجريم الجرائم الإلكترونية والتعريف بنوعية الأدلة إعمالاً لمبدأ شرعية الجرائم والعقوبات حتى نصل إلى إقامة بنية قانونية للتصدي لمثل هذا النوع من الجرائم.
2. ضرورة اهتمام المصارف بالشركات التجارية التي تتعامل ببطاقة الائتمان الإلكترونية بالوقوف على كل طرق وأساليب الاحتيال والخداع والتزوير في الاستخدام غير المشروع لبطاقة الائتمان الإلكترونية مع ضرورة تدريب الموظفين والعاملين على كل ما يستجدّ في هذا المجال وذلك بإقامة برامج تدريبية مكثّفة لموظفي المصارف. وضرورة إعداد برامج إلكترونية دقيقة يمكن من خلالها أن يشفر حامل البطاقة رقم بطاقته بنفسه ويرسله إلى التاجر المعتمد، والذي بدوره يستطيع فكّ التشفير، وذلك منعًا لاختراق المعلومات المصاحبة لاستخدام بطاقة الائتمان عبر شبكة الإنترنت.
3. التعريف بالمنظومة الحكومية التي يلجأ إليها المستهلك للتأكّد من مصداقية مواقع التسوق الإلكتروني، ووجود رقابة على المتاجر الإلكترونية بكافة أنواعها وعدم الشراء عن طريق الإنترنت إلا بعد التأكّد من الموقع بالسؤال عنه، والسؤال عن السلعة في أكثر من موقع.
4. عدم فتح الرسائل التي يكون مصدرها غير موثوق، والحذر من الفيروسات التي تخترق بياناتك، وتحميل برنامج حماية على الحاسوب والهواتف الذكية لمنع اختراقها.

5. تعريف الجمهور بنوعية الرسائل غير المرغوب فيها مثل رسائل التسوّل الإلكتروني وانتحال صفة كبار الشخصيات. تجاهل رسائل الفوز بالجوائز واليانصيب، وتجاهل الرسائل التي تطلب المساعدة في تحويل الأموال.
6. وضرورة إيجاد برامج رسمية ومجتمعية توعوية تهدف لتوعية أفراد المجتمع بمخاطر وأنواع الاحتيال الإلكتروني واستخدام برامج وسائل التواصل الاجتماعي في التوعية.

المراجع باللغة العربية والإنجليزية:

1. أحمد، هلالي عبد اللاه (2011م). محاضرات في علم المجني عليه أو ضحايا الجريمة، دار النهضة العربية، القاهرة، مصر.
2. البشري، محمد الأمين (2005م). علم ضحايا الجريمة وتطبيقاته في الدول العربية (الطبعة الأولى)، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية.
3. الحربي،خالد سليم (2011م). ضحايا التهريب البشري من الأطفال، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية.
4. الخن، محمد طارق عبد الرؤوف، (2011)، جريمة الاحتيال عبر الإنترنت (الأحكام الموضوعية والأحكام الإجرائية)، الطبعة الأولى، منشورات الحلبي الحقوقيه، بيروت، لبنان.
5. الدبل، صالح بن عبد الله، (2011م). ضحايا الاعتداءات الجنائية: دراسة نظرية وميدانية على مستوى مناطق المملكة العربية السعودية، مجلة الاجتماعية – الجمعية السعودية لعلم الاجتماع والخدمة الاجتماعية– السعودية.
6. الردايدة، عبد الكريم خالد، (2006م). دور أجهزة العدالة الجنائية في حماية حقوق ضحايا الجريمة دراسة مقارنة ما بين القوانين الوضعية والشريعة الإسلامية، جامعة عمان العربية، الأردن.

7. السلحدي، سيف راشد، (2014م) الجوانب الموضوعية لجريمة الاحتيال الإلكتروني (دراسة مقارنة)، إدارة الدراسات العليا، كلية الشرطة، وزارة الداخلية، الإمارات.
8. العمر، معن خليل (2009م). علم ضحايا الإجرام، دار الشروق، عمان.
9. العنزي، ممدوح رشيد محمد الرشيد، (2016م). الحماية الجنائية للمجني عليه من الابتزاز، المجلة العربية للدراسات الأمنية والتدريب (السعودية).
10. العموش، أحمد فلاح، (2003م)، الخوف من الجريمة في مجتمع الإمارات، الشارقة، مركز البحوث والدراسات.
11. العموش، أحمد فلاح (2008م). المشكلات الاجتماعية في مجتمع الإمارات: دراسة ميدانية من وجهة نظر المبحوثين، مجله العلوم الاجتماعية، الكويت.
12. الفيل، علي عدنان، (2012م)، جريمة الاحتيال عبر البريد الإلكتروني، دراسة مقارنة، مجلة الحقوق (الكويت)، مج 36، ع 2.
13. الفالح، سليمان قاسم، (2006م)، مخاطر جرائم الاحتيال، الحلقة العلمية (تكامل جهود الأجهزة الأمنية والعدلية في مكافحة جرائم الاحتيال)، كلية التدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية.
14. المطيري، محمد بن غالي بن فهد، (2008م)، خصائص ضحايا جرائم الاحتيال المالي على عينة من الضحايا بمدينة الرياض، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية.
15. المنشاوي، محمد (2002م) جرائم الإنترنت في المجتمع السعودي: رسالة ماجستير غير منشورة، قسم.

16. جاسم،محمد علي سالم، (2015م)، حماية حقوق ضحايا الجريمة في مرحلة التحقيق الابتدائي، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع.
17. مجمع البحوث والدراسات، (2016م). الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، أكاديمية السلطان قابوس لعلوم الشرطة، نزوى، عمان.
18. هلال، ناجي محمد (2005م) التحليل الاجتماعي لضحايا الجريمة، مركز بحوث الشرطة، شرطة الشارقة، الإمارات.
19. هلال، ناجي محمد سليم (2012م). ضحايا الجريمة: دراسة اجتماعية على عينة من ضحايا جرائم السرقة، مصر.
20. يوسف، صغير، (2013م)، الجريمة المرتكبة عبر الإنترنت، رسالة ماجستير غير منشورة، كلية الحقوق والعلوم السياسية، جامعة مولوود معمري، تيزي وزو، الجزائر.
21. Daigle،leah E (2012) ،Victimology، London SAGE publication
22. Daigle،leah E(2013) ،Victimology، London SAGE publication
23. Daigle،leah E(2018) ،Victimology، London SAGE publication
24. Marcum,Catherin(2014).cyber crime ,New York,Wolters Kluwer Law & Business
25. National Crime Victimization survey، 2017، Bureau of Statistics، U.S Department of Justice، office of justice programs

26. William H. Sousa، Ph.D. (2004). “Broken Windows” Crimology and Criminal Justice، University of Nevada Las Vegas

27. Williams III، Frank and Marilyn D.McShane (2010) . Criminological Theory، Pearson Education.

الملاحق

الملحق (1): الاستبيان.
الملحق (2): كتاب من الجامعه للدوائر الحكومية والخاصة.
الملحق (3): المقابلات.

الملحق (1): الاستبيان.

بسم الله الرحمن الرحيم

أخي العزيز/ أختي العزيزة

السلام عليكم ورحمة الله وبركاته

يتناول هذا البحث موضوع ضحايا الاحتيال الإلكتروني في المجتمع الإماراتي، وما ستدلون به من معلومات، يمثّل أساس البحث للتوصل إلى الحقائق العلمية المتعلّقة بموضوع البحث بهدف وضع برنامج وقائي للحدّ من ظاهرة الاحتيال الإلكتروني لذا أرجو التجأوب في هذا البحث والتزام الدقة والصراحة في تعبئة بيانات الاستبيان ونؤكد سرية المعلومات، وأن المعلومات لن تستخدم إلا لأغراض البحث العلمي

الباحثة ناهد علي سيار
U16101567

البيانات الأولية						
العمر	أقل من 18	من 18– أقل من 30	30– أقل من 40	40 – أقل من 50	50 – أقل من 60	60 فأكثر

الجنس	ذكر	أنثى

الحالة الاجتماعية	متزوج	أعزب	مطلق	أرمل

الجنسية	إماراتي	دول مجلس التعاون	غير ذلك: (الرجاء التحديد)

محل الإقامة	عجمان	الشارقة	أم القيوين	دبي	أبوظبي	الفجيرة	رأس الخيمة
المستوى التعليمي	أمي	يقرأ ويكتب	ابتدائي	إعدادي	ثانوي	بكالوريوس	دراسات عليا

المهنة	طالب	قطاع حكومي	قطاع خاص	أعمال حرة	قطاع شبه حكومي	لا يعمل

الدخل الشهري	أقل من 10.000	من 10.000 إلى أقل من 20000	من 20.000 إلى أقل من 30000	30.000 فأكثر

مصدر الدخل	عمل	تجارة	عقارات	معاش تقاعد	عمل الزوجة	من الجمعيات الخيرية	أخرى:

المسكن	شقة	فيلا	بيت شعبي	أخرى:

البيانات التقنية الأساسية		
أنواع الهواتف الجوالة التي تستخدمها	الهواتف الذكية	الهواتف التقليدية

المدة الزمنية التي تقضيها في استخدام الهواتف الجوالة	أقل من ساعة	من ساعة إلى أقل من ساعتين	من ساعتين إلى 3 ساعات	ساعات فأكثر

شبكات التواصل الاجتماعي التي تستخدمها	تويتر	فيس بوك	سناب شات	أنستجرام	كل ما سبق	أخرى حدد:

المدة الزمنية التي تقضيها في استخدام شبكات التواصل الاجتماعي	لا أستخدمها نهائيًا	أقل من ساعة	من ساعة إلى أقل من ساعتين	من ساعتين إلى 3 ساعات	3 ساعات فأكثر

ما هي صور الاحتيال الإلكتروني الشائعة في المجتمع؟			
سوق العملة الإلكتروني (بيع العملة الافتراضية)	موجود	غير موجود	لا أعلم
الاحتيال الإلكتروني عن طريق موظّفي المصارف	موجود	غير موجود	لا أعلم
الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان	موجود	غير موجود	لا أعلم
تزوير بطاقة الائتمان	موجود	غير موجود	لا أعلم
الاحتيال الإلكتروني التجاري وذلك من خلال التسوق الإلكتروني	موجود	غير موجود	لا أعلم
الاحتيال الإلكتروني عن طريق الشركات	موجود	غير موجود	لا أعلم
الاحتيال عن طريق المحافظ الاستثمارية الوهمية الإلكترونية	موجود	غير موجود	لا أعلم
الاحتيال عن طريق الإعلان عن الوظائف الوهمية	موجود	غير موجود	لا أعلم
انتحال صفة كبار الشخصيات (ما انتشر بالفترة الماضية عن طريق وسائل التواصل الاجتماعي بانتحال بعض الشخصيات لصفة الشيوخ وطلب تحويل أموال لهم)	موجود	غير موجود	لا أعلم
التسول الإلكتروني (ادعاء أشخاص للفقر عن طريق وسائل التواصل الاجتماعي وهم ليسوا فقراء)	موجود	غير موجود	لا أعلم
الاحتيال الإلكتروني العاطفي: عندما يبني المحتال علاقة قوية على الإنترنت مع شخص ما ويتم إقناع الضحية بالقيام بإرسال صوره فيقوم المحتال بطلب أموال لعدم نشر الصور على الإنترنت.	موجود	غير موجود	لا أعلم
الاحتيال والنصب عبر الهاتف	موجود	غير موجود	لا أعلم
الاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي، وذلك عن طريق اختراق برامج التواصل الإجتماعي وطلب أموال من أصدقاء الضحية	موجود	غير موجود	لا أعلم
الاحتيال الإلكتروني عن طريق اليانصيب	موجود	غير موجود	لا أعلم

هل سبق أن تعرّضت للاحتيال الإلكتروني	نعم	لا

صور الاحتيال الإلكتروني	إذا كنت قد تعرضت فما هي صور الاحتيال الإلكتروني التي تعرضت لها شخصيًّا		
	أقل من 12 شهر	منذ سنتين	أكثر من 3 سنوات
سوق العملة الإلكتروني (بيع العملة الافتراضية)			
الاحتيال الإلكتروني عن طريق موظّفي المصارف			
الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان			
تزوير بطاقة الائتمان			
الاحتيال الإلكتروني التجاري وذلك من خلال التسوق الإلكتروني			
الاحتيال الإلكتروني عن طريق الشركات			
الاحتيال عن طريق المحافظ الاستثمارية الوهمية الإلكترونية			
الاحتيال عن طريق الإعلان عن الوظائف الوهمية			
انتحال صفة كبار الشخصيات			
التسول الإلكتروني			
الاحتيال العاطفي			
الاحتيال والنصب عبر الهاتف			
الاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي			
الاحتيال الإلكتروني عن طريق اليانصيب			

هل سبق أن تعرض أحد أقاربك أو أصدقائك للاحتيال الإلكتروني	☐ نعم	☐ لا

صور الاحتيال الإلكتروني	إذا قد تعرض أحد أقاربك وأصادقك فما هي صور الاحتيال الإلكتروني التي تعرضوا لها		
	أقل من 12 شهر	منذ سنتين	أكثر من 3 سنوات
سوق العملة الإلكتروني (بيع العملة الافتراضية)			
الاحتيال الإلكتروني عن طريق موظّفي المصارف			
الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان			
تزوير بطاقة الائتمان			
الاحتيال الإلكتروني التجاري وذلك من خلال التسوق الإلكتروني			
الاحتيال الإلكتروني عن طريق الشركات			
الاحتيال عن طريق المحافظ الاستثمارية الوهمية الإلكترونية			
الاحتيال عن طريق الإعلان عن الوظائف الوهمية			
انتحال صفة كبار الشخصيات			
التسول الإلكتروني			
الاحتيال العاطفي			
الاحتيال والنصب عبر الهاتف			
الاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي			
الاحتيال الإلكتروني عن طريق اليانصيب			

بعد تعرضك للاحتيال الإلكتروني أو بعد تعرض أحد أصدقائك أو أقربائك تم إبلاغ:					
الأسرة	الأصدقاء	الشرطة	لم أبلغ أحد	كل ما سبق	أبلغت أشخاصًا آخرين: ((الرجاء التحديد):
إذا لم تبلغ أحدًا/ ما هي الأسباب؟	الخوف من سخرية الآخرين	عدم اهتمامي بالمبلغ	قناعتي بأن القانون لا يحمي ضحايا الاحتيال الإلكتروني	أخرى:	

القانون وضحايا الاحتيال الإلكتروني		
هل قمت بالاطلاع على المواد القانونية التي تتعلق بالاحتيال الإلكتروني في مرسوم مكافحة جرائم تقنية المعلومات؟	☐ نعم	☐ لا

إذا كنت قد اطلعت على المواد القانونية التي تتعلق بالاحتيال الإلكتروني في مرسوم مكافحة جرائم تقنية المعلومات الرجاء الإجابة على الأسئلة الآتية:			
هل تعتقد أن القانون يحمي ضحايا الاحتيال الإلكتروني؟	نعم	لا	لا أعلم
بعد تعرضك للاحتيال الإلكتروني هل أوجد القانون طريقة تكفل حقّك؟	نعم	لا	لا أعلم
هل تعتقد أن هناك قواعد وتشريعات تحمي ضحايا الاحتيال الإلكتروني؟	نعم	لا	لا أعلم
عدم تعاون الضحايا في الإبلاغ عن عمليات الاحتيال الإلكتروني أدى إلى زيادتها؟	نعم	لا	لا أعلم
عدم تناسب العقوبة التي توقع على الجناة أدى إلى عدم الإبلاغ عن جرائم الاحتيال الإلكتروني؟	نعم	لا	لا أعلم

التسوق الإلكتروني		
هل تتسوق إلكترونيًّا	نعم	لا

هل هذه العوامل تؤدي إلى تعرض الضحية للاحتيال الإلكتروني؟			
إهمال الضحايا في التعامل مع بياناتهم الشخصية	نعم	لا	لا أعلم
عدم الوعي بأساليب الاحتيال الإلكتروني يزيد من جرائم الاحتيال الإلكتروني	نعم	لا	لا أعلم
الجهل بالتدابير الأمنية لدى المستهلك (الحيطة والحذر من الوقوع ضحية للاحتيال الإلكتروني)	نعم	لا	لا أعلم
الثقة الزائدة لدى المستهلك (الدفع قبل الاستلام)	نعم	لا	لا أعلم
عدم إبلاغ الضحايا عن تعرضهم للاحتيال الإلكتروني	نعم	لا	لا أعلم

إذا كنت تتسوق إلكترونيًا فما طريقة الدفع التي تفضلها مع تحديد السبب؟					
الدفع بعد الاستلام		الدفع المسبق عن طريق بطاقة الدفع الإلكتروني			
إذا اخترت الدفع بعد الاستلام هل بسبب؟	خوفًا من عدم مطابقة البضاعة للمواصفات	خوفًا من عدم وصول البضاعة	كل ما سبق		أسباب أخرى حددها:
إذا اخترت الدفع المسبق عن طريق بطاقة الدفع الإلكتروني هل السبب؟	لسهولة إنجاز المعاملة	بسبب الخصم الذي يعطى على البضاعة في حالة الدفع قبل الاستلام	الثقة الزائدة	كل ما سبق	أخرى :

الملحق (2)

كتاب من الجامعة للدوائر الحكومية والخاصة

جامعة الشارقة
UNIVERSITY OF SHARJAH

كلية الآداب و العلوم الإنسانية و الاجتماعية
قسم علم الاجتماع

College of Arts, Humanities & Social Sciences
Department of Sociology

التاريخ : 2018/5/10

لمن يهمه الامر

تحية طيبة ،،،

م / تسهيل مهمة

بداية نهديكم أطيب التحيات متمنين لكم دوام التوفيق والنجاح لما تبذلونه من جهود من أجل خدمة المجتمع من خلال التعاون المثمر مع جامعة الشارقة . وبالإشارة إلى الموضوع أعلاه يرجى التكرم بتسهيل مهمة الطالبة ناهد علي سيار بتوزيع استبيان تحت عنوان : ضحايا الاحتيال الالكتروني في المجتمع الاماراتي للاستفادة من المعلومات وتوظيفها في مساق الرسالة علمًا بأن هذه البيانات تستخدم فقط لأغراض البحث العلمي .

وتفضلوا بقبول فائق الاحترام

كلية الآداب والعلوم الإنسانية والاجتماعية – قسم علم الاجتماع – جامعة الشارقة UNIVERSITY OF SHARJAH – Dept. of Sociology – College of Arts, Humanities & Social Sciences

ا.د.نايف البنوي

رئيس قسم علم الاجتماع

هاتف: ٣٢٢٤ ٥٠٥ ٦ (٩٧١+) فاكس: ٥٠٥٣٢٦٦ ٦ (٩٧١+) ص.ب: ٢٧٢٧٢، الشارقة – الإمارات العربية المتحدة
Tel : (+971 6) 505 3224, Fax: (+971 6) 5053266, P.O. Box : 27272, Sharjah - United Arab Emirates
E-mail: sociology@sharjah.ac.ae www.sharjah.ac.ae

الملحق (3): المقابلات

عرض نتائج الدراسة الكيفية:

تم الحصول على هذه النتائج من خلال إجراء المقابلات مع بعض الحالات التي قابلتها الباحثة، وتمكّنت من إجراء المقابلات أثناء تعبئة الاستبيان وبعض المقابلات في وقت آخر حرصًا منها على الحصول على أكبر قدر من المعلومات، وتم إجراء 42 مقابلة.

الاحتيال عبر بيع العملة الافتراضية	
الحالة الأولى	شاب من الجنسية السودانية يبلغ من العمر 35 سنة يذكر أنه تم خداعه عن طريق البتكوين بأنه سيضمن دخلا شهريا له، وأنه سيتم مضاعفة أمواله. فيذكر أنه دخل البتكوين بمبلغ 30000 وسرعان ما تم سرقة المبلغ، وإيهامه بأنه تم خسارته أثناء التداول ولم أستطع الإبلاغ بسبب قناعتي أن القانون لا يحمي الضحايا، ولا أملك أيّ دليل.
الحالة الثانية	امرأة سورية تبلغ 30 سنة تذكر أنه تم الاحتيال عليها عن طريق إعلان عبر موقع تداول فيرفوكس وتم إيداع عشر آلاف وبأقل من شهر خسرت المبلغ بالكامل وتم إبلاغ الشرطه لكن لا فائدة.
الاحتيال عن طريق موظّفي المصارف:	
الحالة الثالثة	رجل إماراتي يبلغ من العمر 38 سنة يذكر عن الاحتيال عن طريق موظفي المصارف بأنه سيتم استقطاع مبلغ معين لمدة 20 سنة، فالبنك يستقطع من الشخص بشكلٍ عادي لمدة 5 سنوات ومن بعدها تضاف مبالغ أخرى يتم الاحتيال بها، ويتم من خلالهم إجبار العميل دفع المبالغ المالية شهريًّا غير العقد الذي أبرمه أول مرة.

الاستيلاء على الأموال عن طريق سرقة بيانات بطاقة الائتمان:	
الحالة الرابعة	فتاة إماراتية تبلغ من العمر 28 سنة ذكرت أنه تم الاتصال بها هاتفيًا والادعاء أنها ربحت مبلغ 100 ألف درهم، وتم سؤالها إذا قد شاركت في أحد السحوبات وكانت بالفعل قد شاركت في السحب فأجابت نعم، فقالوا إنها ربحت 100 ألف درهم وإنهم يريدون رقم حسابها للتحويل، وأرادوا بيانات أخرى فأعطتهم بحسن نية فتم سحب رصيدي من البنك حيث بلغ المبلغ 50000 درهم، وتم سحبه بالكامل وقامت بالإبلاغ، لكن للأسف دون جدوى لأنه لا يوجد لديها دليل، وأيضًا تم سحب المبلغ فلا يمكن استرجاعه.
الحالة الخامسة	شاب إماراتي يبلغ من العمر 31 سنة، يذكر أنه أثناء تسوقه عن طريق الإنترنت تم سحب مبلغ أقصى من البطاقة فقام بإبلاغ البنك وقاموا بإيقاف البطاقة.
تزوير بطاقة الائتمان	
الحالة السادسة	شاب إماراتي عمره 37 سنة يذكر أنه من خلال تقديم لوظيفة عن طريق النت تم استغلال البيانات الشخصية في استخراج بطاقات ائتمان بمساعدة من قبل موظف في البنك باسمي.
الاحتيال بوجود مشروع كاذب	
الحالة السابعة	رجل أعمال من دول مجلس التعاون يبلغ من العمر 32 سنة تعرض للاحتيال الإلكتروني من عصابة تستهدف رجال الأعمال: فتقوم بخداعه بوجود مشروع مع الإغراء بحيث يقولون له إن لدينا رأس المال ولكننا جديدون بالسوق، فيكون المشروع باسمك لأنك تاجر معروف، وسيكون رأس المال منا 70 % ومنك 30%، أما الأرباح فستكون لك 70% ولنا 30%، فعندما رأى التاجر هذه الصفقة التي تعتبر ناجحة وتأكد من كلامهم قام بتحويل المبلغ وقدره 200 ألف، واتضح له بعد ذلك أنه قد تعرض ضحية لعصابة تعمل على النصب على رجال الأعمال وتسلب أموالهم وتوظّفها في غسيل الأموال، فالآن لا يستطيع الإبلاغ لأنه يعتبر أحد المساهمين في الجريمة ولا يستطيع أن يتوقف أو يصمت لأنه يتم ابتزازه إذا لم يستمر معهم سيتم الإبلاغ عنه. فهذه في البداية كانت جريمة مالية وبعدها تحوّلت إلى جرائم مركبة دخل فيها غسيل الأموال والابتزاز وغيرها من الجرائم الأخرى.
الاحتيال الإلكتروني التجاري	
الحالة الثامنة	رجل إماراتي متزوج يذكر الحادثة ويقول: قمت بشراء خاتم لزوجتي على أنه ألماس من الأنستغرام وبعدها اكتشفت بأن الخاتم ليس ألماسًا.

الحالة التاسعة	ذكر إماراتي يبلغ من العمر 25 سنة أنه اشترى عن طريق موقع أنستجرام آثاث بيت، وتم تحويل المبلغ وبعد ذلك لم يتم استلام الآثاث.
الحالة العاشرة	شاب إماراتي يبلغ من العمر 26 سنة يقول: قمت بشراء سيارة كلاسيك من موقع ebay ولكن تم النصب علي ولم أستلم السيارة، أبلغت الشرطة ولكن دون جدوى لأنه خارج الدولة.
الحالة الحادية عشر	فتاة إماراتية تبلغ من العمر 32 سنة تذكر أنها قامت بشراء سيارة فارهة عن طريق موقع مزور لموقع معروف وتم تحويل المبلغ قبل الاستلام.
الحالة الثانية عشر	شاب مصري 23 سنة يذكر أنه اشترى هاتفًا عن طريق الإنترنت، واتّضح بعد ذلك أنه (صيني) تقليد، وذهب إلى مراكز الشرطة إلى أن وصلت إلى مركز الجرائم الإلكترونية وفي النهاية قال لي الشرطي المسؤول حرفيًّا (ما عندك دليل أن الي باعك التلفون باعك تلفون نقلي .. حتى لو مسكناه بيقول أنا عطيتك تلفون أصلي.. اتهنى بيه !).
الحالة الثالثة عشر	رجل من دول مجلس التعاون يبلغ من العمر 25 سنة يذكر أنه طلبت من موقع إلكتروني بطاريات بكميات كبيرة ومدعين بأنها أصلية وعندما وصلتني اكتشفت أنها غير أصلية وغير قابلة للشحن، ومرة أخرى طلبت أشرطة سوني وعندما وصلتني لم يكن هناك أشرطة فقط الغلاف.
الحالة الرابعة عشر	أنثى متزوجة من الإمارات تبلغ من العمر 43 سنة ذكرت الحالة أنها اشتريت من تاجرة في الكويت غرضًا معيّنًا، ولم ترسله لها ودفعت لها المبلغ كاملاً عن طريق التحويل من محل الصرافة ولم ترسل لي الغرض ولم ترجع لي مالي ولا زالت موجودة على الأنستقرام وتبيع ولم أعلم أين أذهب فوكلت أمري إلى الله.
الحالة الخامسة عشر	فتاة تبلغ من العمر 20 سنة إماراتية ذكرت أنها تعرضت للاحتيال عن طريق التسوق الإلكتروني (البضاعة لم تكن كما في العرض وأيضًا السعر مرتفع جدًّا)، وتم إبلاغ حماية المستهلك، كما تم التواصل مع السوق الإلكتروني نفسه، وأيضًا تم سرقة بيانات البطاقة الائتمانية عن طريق اتصال هاتفي والاستيلاء على الأموال، وكذلك إبلاغ البنك لإيقاف البطاقة.

الاحتيال عن طريق الشركات	
فتاة إماراتية 30 سنة تذكر أنها تعرضت للاحتيال من قبل شركات وهمية لبيع الشقق وكانت هذه الشركات تقوم بعمل احتفال كبير وحضور شخصيات مهمّة في الحضور عندما يحضر هذا الكم الهائل يتصور أن الشركة ناجحة ويوثق بهم، وعندما يتم تقديم الدفعَة الأولى يتم انسحاب الشركة واختفاؤها نهائيًّا.	الحالة السادسة عشر
أنثى إماراتية تبلغ من العمر 27 سنة تذكر قصة أحد أقاربها جاءها اتصال من شركة، وألحّوا على إعطائها رقم البطاقة البنكية وأنها لن تسحب المبلغ، ومن ثم تم سحب المبلغ فورًا بعد المكالمة على أنها وافقت لكنها لم توافق وبعدها طالبت برد المال! قالت لها الشركة إنها سترسل بعض الأوراق لكي توقع ويتم استرداد المبالغ كامل، وبما أن العقد كان بالإنجليزية، وهي لا تعرف الإنجليزية وقعت دون فهم العقد، ثقة بما قالته لها صاحبة الشركة، بعدها قالوا لها إنها وقعت على أنها موافقة على الاشتراك وهكذا تم النصب عليها، وذهبنا للشرطة لكن لم نستفد شيئًا.	الحالة السابعة عشر
فتاة تبلغ من العمر 43 من الجنسية البريطانية متزوجة ذكرت أنه تم إعطاء بيانات البطاقة لشركة معروفة في قطاع السياحة ولكن لم تتم إعطاؤهم الموافقة على سحب أيّ مبلغ قبل إخطارها بذلك. وقامت الشركة بسحب أقصى من حساب البنك مما اضطرها أن تغيّر البطاقة الائتمانية لتفادي حدوث أيّ سرقة مرة أخرى. الحادث الثاني الشراء عبر الإنترنت من موقع متداول وحين تأخر استلام الطلبية حاولت التواصل مع الشركة ولكن دون جدوى، واتّضح من البحث أنها شركة ذات سمعة سيئة، وسبق أن خدعت كثيرًا من المتعاملين، وتقول إنها لم تقم بالإبلاغ بسبب قناعتها بأن القانون لا يحمي المغفلين فلهذا فقط اكتفيت بإلغاء البطاقة ولم أبلغ سوى أسرتي وأصدقائي.	الحالة الثامنة عشر
رجل مصري يبلغ 35 سنة يذكر أنه تم الاتصال به من شركة تدعي أنها على خبرة طويلة في البورصة، وتطلب من العملاء الاشتراك معهم وتدريبهم عبر الهاتف، والموقع الخاص بهم مقابل حساب وهمي في بادئ الأمر ثم يطلبون من الضحية تحويل مبلغ من المال، وبعد ذلك يبلغونه أنه تمت خسارة المبلغ في البورصة، وأيضًا تعرّض لعملية نصب أخرى من قبل شركة وهمية تعد من يشترك معها بالحصول على الجرين كارد للسفر لأمريكا والعمل والدراسة بها مقابل مبالغ من المال.	الحالة التاسعة عشر

الاحتيال العاطفي	
فتاة إماراتية تبلغ من العمر 24 سنة تحكي أنه تم ابتزاز أحد أقاربها وطلب منه دفع مبلغ مالي بعدما كان على تواصل بفتاة وقاموا بعلاقة جنسية على سكايب حيث سجلت محادثة الفيديو وهددت بنشرها للأصحاب والأهل عبر الأنستقرام، وكما نشرتها على يوتيوب ولكن قمنا بعمل ريبورت على الفيديو في يوتيوب، ومسح خلال دقائق. وكذلك قدمنا بلاغاً في الشرطة، والتي أدّت دورها على أكمل وجه وطويت الصفحة، والحمد لله.	الحالة العشرون
فتاة من الجنسية الإماراتية تبلغ من العمر 22 سنة ذكرت الفتاة أنها تعرفت على شاب عن طريق الفيس بوك، وقامت بيننا علاقة عاطفية استمرت لمدة 4 سنوات وفي السنة الخامسة مرض والدها مرضًا شديدًا فبدأ الشاب بابتزازي إذا لم أعطه المال فإنه سيقوم بنشر صوري وإخبار والدي بما بيننا، فخفت وكنت مضطرة لإعطائه المبالغ التي يريدها، ولم أبلغ بسبب قناعتي بأنّ القانون لا يحمي المغفلين، وبسبب خوفي من وصول الأمر لعائلتي، وإلى الآن يقوم بابتزازي في بعض الأوقات.	الحالة الحادية والعشرين
رجل سوداني يبلغ من العمر35 يذكر حالة إحدى الفتيات التي يعرفهن فيقول إنّ هذه الفتاة كانت لديها علاقة عاطفية بشاب وكانت ترسل صورها له، وقام هذا الشاب بإنشـــاء حساب فيس بوك باسمها وبصورها، وقام بإرسال صورها للرجال وعندما علمت واجهته فقام بابتزازها وطلب الأموال مقابل التوقّف عن هذا الفعل.	الحالة الثانية والعشرون
فتاة مصرية تبلغ من العمر 24 سنة تذكر حالة إحدى صديقاتها حيث تقول إنّ صديقتي كانت على علاقة عاطفية بشخص على موقع من المواقع الإلكترونية ادعى فيها أنه يملك منصبًا ونسبًا عاليًا في الدولة. حاولت تحذيرها منه لكن لم تجدي أيّ من الوسائل معها بعد مشاركة صور خاصة لها من قبل هذا الشخص تم تهديدها بها وإرغامها على الاستمرار بنشر صورها له، وإعطائه مبالغ مالية أيضًا... استمر مدة سنة كاملة لكن لم يعلم بالمشكله أيٌّ من عائلتها ولم تبلغ خوفا من سخرية الآخرين ووصول الأمر لعائلتها.	الحالة الثالثة والعشرون
دكتورة في الخدمة الاجتماعية في إحدى الدوائر قابلتها تشير إلى إحدى حالات الاستشارة التي مرّت بها، فتقول هناك حالة فتاة تعرضت للابتزاز العاطفي ولا يمكنها الإبلاغ عن الجاني، وذلك لأنّ القانون يفرض على الضحية أن يبلغ بنفسه عن الجاني، وهذا الأمر لا يمكنها القيام به بسبب وضعها الاجتماعي.	الحالة الرابعة والعشرون

الحالة الخامسة والعشرون	رجل من دول مجلس التعاون يبلغ من العمر 27 سنة من محترفي الهاكرز يذكر حادثة فتاة من دول مجلس التعاون تبلغ من العمر 24 سنة منذ 6 سنوات كالآتي: إنّ الفتاة كانت مضافة لديه في أحد برامج التواصل الاجتماعي ويلاحظ اختفاءها لفترات طويلة ودائما ما تضع صور وعبارات حزينة، ففي يوم من الأيام سألها فأجابته أنه منذ عدة أشهر توفيت عائلتها أمها ووالدها ولم يبق لها أحد وأصبحت هي في سن الـــ18 مسؤولة عن إخوتها الصغار، وكانت على معرفة سطحية بأحد الرجال، ففي هذه الأوقات العصيبه التي مرّت بها وقف معي وكان يقول إنني سأعوضك عن والديك وسأساعدك في الاعتناء بإخوتك، فوجدت فيه طوق النجاة الذي سيخرجها من وضعها ذاك، ومع الأيام أحبّته وأصبحت تقوم بما يطلب وترسل صورها له، وبعد ذلك قامت بالخروج معه وبدأت تشعر أنه يقوم باستغلالها، ويريد أشياء أخرى، فبدأت تمتنع عنه فأصبح يقوم بابتزازها، ويطلب أموالاً بالمقابل ويهددها بأنها إذا لم تخرج معه سينشر صورها، ويصل لمنزلها، ويقوم بتهديدها، فأصبحت تعتزل العالم كما رأيت وتغلق هاتفها، ولا تتحدث مع أي شخص، وتجلس في غرفها حتى لا يصل إليها، وبمجرد أن تفتح الهاتف تجد رسائل التهديد منه. ويقول الرجل طلبت رقم هاتف المبتز وجميع البيانات التي لديها عنه وقمت بالتجمع مع أصدقائي الهاكرز وقمنا باختراق جهازه وسحب جميع الملفات، وبعد ذلك قمنا بالتحدث إلى أصدقائنا وأقاربنا في الأمن وتم تهديده برفع قضية ضده من قبلهم، وبعد ذلك اختفى بشكلٍ نهائي.
الاحتيال عن طريق المحافظ الاستثمارية الوهمية الإلكترونية	
الحالة السادسة والعشرون	رجل إماراتي يبلغ من العمر 34 سنة تعرض للاحتيال عبر موقع www.lesoie.com ويقول إنّ هذا الموقع يقوم بالنصب على المستثمرين الجدد الذين ليس لديهم خبرة. وهو أول موقع يعطي وكالة ويسأل المستثمر كم راتبه؟ وهل لديه خبرة في المشروع من أقاربك حتى يتمكنوا من استغلال المستثمر والاحتيال على أمواله بطريقة قانونية، ويتم خداعه بالأرباح الكبيرة.

الحالة السابعة والعشرون	امرأة مصرية تحكي أنّ أخاها تعرّض للاحتيال الإلكتروني بخداعه بأنه سيحصل على أرباح كبيرة مع بعض الأفارقة، ولكنهم نصبوا عليه في مليون درهم ثم اختفوا وهربوا من البلاد فورًا بعد إيداع المبلغ بحسابهم خارج الدولة.
الاحتيال عن طريق الإعلان عن الوظائف الوهمية	
الحالة الثامنة والعشرون	فتاة من الجنسية الفلسطينية تبلغ من العمر 26 سنة طالبة دراسات عليا، ذكرت أنه تم الإعلان عن وظيفة طلب مترجم فقامت بالعمل معهم والقيام بالترجمة لشهر كامل، وبعد ذلك لم يتم إعطاؤها المبلغ المتفق عليه، ولم تبلغ بسبب قناعتها بأنّ القانون لا يحمي ضحايا الاحتيال الإلكتروني فسألتها: هل أنت على اطلاع على المواد القانونية التي تتعلق بتعرضك للاحتيال الإلكتروني؟ وماهي الوسائل التي يتبعها القانون لاسترجاع حقك؟ أجابت: لا. فقلت: إذن كيف أنت على قناعة بأن القانون لا يحمي الضحايا وأنت غير مطلعة على القانون. فأجابت: لم أكن أعلم بوجود القانون الذي يحمي ضحايا الاحتيال، ولهذا يجب التوعية بوجود هذه القوانين وتعريف الناس بها حتى يتم الإبلاغ في حال تعرّضهم لها.
انتحال صفة كبار الشخصيات	
الحالة التاسعة والعشرون	رجل إماراتي يبلغ من العمر 48 سنة تعرض للاحتيال، ويذكر أنه دخلت عليه شخصية منتحلة إحدى شخصيات بنات الشيوخ، وتقول إنها مسافرة وحسابها البنكي محظور، وهي تساعد عائلة، وتطلب منه أن يقوم بالتحويل بدلاً عنها، وعندها تعود ستقوم بإعطائه أضعاف المبلغ.
التسوّل الإلكتروني	
الحالة الثلاثون	فتاة إماراتية تبلغ من العمر 27 سنة تعرضت للسرقة حيث ادّعت شخصية من جنسية عربية أنها لا تجد قوت يومها وبعد تحويل المبلغ اكتشفت أنها عصابة نصب تستهدف أبناء الخليج، ولم تبلغ بسبب عدم اهتمامها بالمبلغ.
الحالة الحادية والثلاثون	من خلال مقابلتي لإحدى المحاميات في محاكم عجمان ذكرت لي قصة إحدى القضايا، حيث ذكرت أن الحالة رجل إماراتي مسكت قضيته، وقد تعرّض للنصب من خلال شخص ادعى أنه إمرأة ولا تملك قوت يومها، وهو في الواقع رجل وسحب منه مبالغ مالية بسبب الكذب عليه.

الاحتيال والنصب عبر الهاتف	
الحالة الثانية والثلاثون	فتاة مصرية تذكر أنه: تعرض خالها لعملية نصب من شخص ادعى أنه يعمل لدى شركة اتصالات، وأخبره أنه فاز بمبلغ من المال ولكي يستلمه يجب عليه دفع مبالغ صغيرة على دفعات، وقد قام خالي بالدفع حتى وصل المبلغ إلى 9 آلاف درهم ولم يستطع استرداده عندما اكتشف أنها خدعة.
الحالة الثالثة والثلاثون	رجل إماراتي يبلغ من العمر 40 سنة يذكر أنه تعرض للاتصال الوهمي من أحد الأشخاص يدعي بأنه من مؤسسة الاتصال، ويقول بأنني ربحت مبلغًا ماليًا، ويريد تحويل الأموال، وعند التحويل يتضح بأنه ليس من الاتصال وأنني تعرضت للنصب، وعند الإبلاغ لم يتمكن من التوصل إلى الجاني كون الرقم غير معروف المصدر.
الحالة الرابعة والثلاثون	رجل من جنسية عربية يذكر أن صديقه شخصية ذو وظيفة مرموقة ومركز علمي (طبيب) تعرض لواقعة احتيال عبر الهاتف، حيث إنه يجب عليه إرسال مبلغ ليتم إرسال الجائزة، فقام بإرسال مبلغ مالي يقارب الثلاثين ألف درهم، وقام بإبلاغ الشرطة لكن بسبب أنه من دولة أخرى صعب الوصول له.
الحالة الخامسة والثلاثون	رجل إماراتي يقول: إنّ عمتي قالوا لها ربحت مليونين لكن حوّلي 10 آلاف، وحولت لهم، ولم تبلغ لأنها قالت بسبب قناعتي بأن القانون لا يحمي ضحايا الاحتيال الإلكتروني.
الاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي	
الحالة السادسة والثلاثون	رجل من الجنسية الفلسطينية يذكر أنه تعرض لاختراق الواتساب من قبل شخص من المغرب العربي، ويدخل على أصدقائهو يطلب منهم أموالا، فقام 3 من أصدقائه بتصديقه على أنه صديقهم وقام كل شخص بإرسال 5000 درهم للمحتال ظنًا منهم أنه صديقهم فقام أحد الأشخاص بالإيقاع بالمحتال، وقال: أرسل لي اسمك بالكامل لكي أرسل المبلغ، فتم إرسال اسمه بالكامل واستخرج بياناته وصورته وأرسلهم له، وقال له أنا أعرفك وأنت مطلوب للأنتربول، وقام بتهديده فاختفى، ولم يعد يطلب أموالاً من أصدقاء الضحية، وتم الإبلاغ لكن بسبب أنه في دوله أخرى لم يحدث شيء حتى الآن.

الحالة السابعة والثلاثون	فتاة إماراتية تبلغ من العمر 24 سنة ذكرت أنه قد تم اختراق الكمبيوتر الخاص بها، وتأليف المحتالة لها قصة في أحد وسائل التواصل الاجتماعي وأرادت المساعدة، فأرسلت لي رابطًا، وقامت بإدخالي إلى موقع غريب، وطلبت مني أن أضغط على هذه الغرفة في الدردشة لكي أنادي صديقتها التي كانت موجودة في هذه الغرفة، وهكذا تم اختراق جهازي وسرقت المعلومات والصور وكل ما هو موجود فيه، وتم ابتزازي بها وإلى الآن لم أخبر أحدًا عن هذا الشيء، لأنه يسبّب لي الحرج، ولم أبلغ الشرطة بسبب قناعتي أن القانون لا يحمي ضحايا الاحتيال الإلكتروني.
الحالة الثامنة والثلاثون	امرأة سودانية تبلغ من العمر 55 سنة تذكر أنها: تعرضت لاختراق الفيس بوك وهو على رقمي الذي تم أخذه من جهة الاتصال نتيجة تأخري في سداد الفاتورة فأبلغت الشرطة ولم تتم متابعة قضيتي، وهذا يجعل الجناة في راحة لعدم التتبع والملاحقة، وذلك يزيد من طرق النصب واختراع طرق جديدة له في وسائل التواصل الاجتماعي.
الحالة التاسعة والثلاثون	ذكر إماراتي يبلغ من العمر 31 سنة عن صديقه: أنه تم قرصنة الواتساب الخاص به.. ومن ثم تم التواصل مع جهات الاتصال لديه لطلب المال منتحلاً شخصية صاحب الهاتف. وقد خاطبني اللص لكي أرسل له المال ولكنني استغربت طريقة الحوار واستغربت أكثر من طلب المال مني. فأخذت أماطله حتى تواصلت مع صاحب الهاتف لأبلغه عن الخبر.
الاحتيال الإلكتروني عن طريق اليانصيب	
الحالة الأربعون	فتاة إماراتية تبلغ من العمر 26 سنة تذكر أنه: تم طلب تحويل مبلغ مالي مقدم عن طريق الصرافة لفوزه بجائزة ذهبية، وقمت بالتحويل وبعد ذلك اكتشفت أنه عملية نصب.
الحالة الحادية والأربعون	شاب عربي 37 سنة يذكر أنه طلب منه مبالغ مالية لسداد ضرائب لكونه قد فاز بجائزة يانصيب عن طريق الإنترنت.
الحالة الاثنتان والأربعون	فتاة إماراتية 45 سنة تذكر عن أحد أقاربها فتقول: من خلال الاحتيال عن طريق الفوز باليانصيب والحالة النفسيه للشخص حيث إنه كبير في السن، وتم الاحتيال عليه بسهولة.. ولكن المشكلة أن هذا الشخص لم يتعلم من خطئه ولا يزال يرسل المبالغ حتى بعد أن تم نصحه من قبل الشرطة وبعد أن فشل أبناؤه في ذلك.